UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 1:23-md-03083-ADB-PGL
This Document Relates To: C.A. No. 1:24-cv-11807-ADB BEN MORRIS, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION; ERNST & YOUNG LLP; and BANK OF AMERICA CORPORATION, Defendants.	**FIRST AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND** [Leave to file granted on April 17, 2026, ECF No. 1784]

Plaintiff Ben Morris ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, brings this First Amended Class Action Complaint against Defendants Progress Software Corporation ("PSC"), Ernst & Young LLP ("EY"), and Bank of America Corporation ("BOA"), (collectively with PSC, "Defendants"), and in support thereof alleges as follows:

NATURE OF ACTION

1. This Complaint is being directly filed into this MDL proceeding pursuant to the Court's MDL Order No. 12.

2. Plaintiff incorporates the allegations contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

3. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated customers' Personally Identifiable Information ("PII"). According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

4. As used throughout this Complaint and previously defined in the paragraph above, "PII" is further defined as all information exposed by the data breach ("Data Breach"), including all or any part or combination of first and last name, address, financial account information, debit or credit card numbers, Social Security Numbers and government issued ID numbers.

PARTIES

5. Plaintiff Ben Morris is, and was at all relevant times, a resident and citizen of New Haven, Connecticut.

6. Defendant PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

7. Defendant Ernst & Young LLP is a limited liability partnership organized under the laws of the State of Delaware with its principal place of business located at One Manhattan West, New York, NY 10001[1].

[1] Under the Class Action Fairness Act ("CAFA"), an unincorporated entity does not take the citizenship of all members but instead is considered "a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. §1332(d)(10); *BRT Management LLC v. Malden Storage LLC*, 68 F.4th 691, 696 n. 7 (1st Cir. 2023).

8. Defendant Bank of America is a Delaware corporation with its principal place of business located at 100 North Tryon Street, Charlotte, NC 28255.

JURISDICTION

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendants.

10. Absent the Court's MDL Order No. 12 (Direct Filing Order), Plaintiff would have filed his action in the United States District Court for the Southern District of New York. That court has general jurisdiction over Defendant EY because EY's headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with EY in that district and Plaintiff's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. That court has specific jurisdiction over BOA because BOA purposefully availed itself of the privilege of conducting business with EY in that district and Plaintiff's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Southern District of New York pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in that district.

FACTUAL ALLEGATIONS

Nature of the Relationship between Defendants.

11. EY offers individuals and businesses a variety of business solutions, including but not limited to assurance, consulting, strategy, and tax.

12. BOA is a national bank which provides services to individuals and businesses.[2] In terms of individual services, BOA offers checking and savings accounts, credit cards, home and auto loans, investing services, and tips to improve money habits.[3]

13. One of the clients that EY provides services to is BOA.[4] Those services include, consulting, advising, and tax services. As part of the provision of these services, BOA entrusted the PII of certain of its customers to EY, which included *inter alia*, customers' first and last names, addresses, financial account information, debit or credit card numbers, Social Security Numbers and government issued ID numbers.[5]

14. EY recognizes that it is responsible for ensuring the protection of the PII it is entrusted. EY has published a brochure which outlines all the security measures it purports to implement.[6] In that brochure, EY states that it "believes that a strong business reputation depends on a robust data protection and information security program" and further states that it "views data protection and information security as fundamental components of doing business."[7]

15. EY further boasts the skills of its security team, which "protect[s] information assets, personal data and client information whenever and wherever they are created processed, transmitted or stored,"[8]

16. EY also lays out the steps it purports to take to secure the information of its clients, adhering to an integrated data protection and information security strategy that includes:

---

[2] *Our company*, Bank of America, https://about.bankofamerica.com/en/our-company/what-we-offer, (last accessed July 1, 2024).
[3] *Personal*, Bank of America, https://www.bankofamerica.com/, (last accessed July 1, 2024).
[4] Vilius Petkauskas, *EY breach exposes Bank of America customer credit card numbers*, cybernews (November 15, 2023), https://cybernews.com/news/ey-bank-of-america-data-breach/.
[5] *Id.*
[6] *Protecting your data: EY approach to data protection and information security*, Ernst & Young
[7] *Id.*
[8] *Id.*

"[s]ubject[ing] the global applications and systems to both data privacy impact assessments and security certification reviews;" "[p]rotect[ing] personal data within the EY network using appropriate physical technical and organizational security measures;" and "[c]onfirm[ing] that contracts with third-party processors contain provisions that clients are commensurate with EY policies, practices and controls to confirm that client data is managed properly and securely."[9]

17. BOA similarly recognizes that it is responsible for ensuring the protection of the PII it is entrusted. BOA states that it "regards the confidentiality, security and protection of your personal and financial information as our highest priority. We value your trust and we understand that handling your financial information with care is one of our most important responsibilities."[10] BOA further purports to "have multiple layers of security in place to protect clients, employees and our company"[11]

18. In its security statement, BOA also states that consumer security is "our top priority"[12] and that it "conduct[s] regular assessment reviews and abide[s] by rigorous privacy standards to ensure personal information [it] collect[s], use[s] and share[s] is protected."[13]

19. Yet, contrary to EY's and BOA's data privacy and security representations – by virtue of EY's admissions that it experienced a Data Breach, which revealed the PII of at least 30,000 individuals – EY did not have adequate measures in place to protect and maintain sensitive

---

[9] *Id.*

[10] *Protecting & Sharing your Information FAQs*, Bank of America, https://www.bankofamerica.com/security-center/faq/protecting-information/ (last visited July 10, 2024).

[11] *Id.*

[12] *Bank of America Security Center*, Bank of America, https://www.bankofamerica.com/security-center/overview/ (last accessed July 1, 2024).

[13] *Bank of America U.S. Online Privacy Notice*, Bank of America, https://www.bankofamerica.com/security-center/online-privacy-notice/ (last accessed July 1, 2024).

PII entrusted to it and BOA did not ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected consumers' PII that it shared with third-party service providers and vendors such as EY and with PSC through EY's use of MOVEit. Instead, BOA and EY's privacy statements wholly fail to disclose the truth: that both BOA and EY lack sufficient processes to protect the PII that is entrusted to them.

Defendants Failed to Protect Plaintiff's and Class Members' PII.

20. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of their IT vendors' and affiliates' data security practices and systems. Defendants had a legal duty to keep PII safe and confidential.

21. Defendants had obligations created by the Federal Trade Commission Act ("FTCA"), contract, industry standards, representations made to Plaintiff and Class Members, and common law to keep their PII confidential and to protect it from unauthorized access and disclosure.

22. 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.

23. 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.

Plaintiff's Experience with the Data Breach.

24. Plaintiff, at all relevant times, was a customer of Defendants BOA and EY.

25. In order for Plaintiff to obtain Defendants' services, Plaintiff was required to provide his PII, directly or indirectly, to Defendants, including his name, date of birth, address, email address, phone number, and other sensitive information.

26. At the time of the Data Breach, Defendants retained Plaintiff's PII in its servers and shared it with its vendors and service providers.

27. Plaintiff received a Notice Letter by U.S. mail, which informed him that his PII had been implicated in the Data Breach.

28. As a result of the Data Breach, Plaintiff has changed the passwords to his accounts and monitored his financial information. Despite his efforts, Plaintiff found multiple fraudulent charges, totaling over $1,200.00 and was hacked twice.

29. As a result of these fraudulent charges, Plaintiff was unable to make a car insurance payment, and had his policy cancelled by the insurer.

30. The Data Breach caused Plaintiff to suffer fear, anxiety, and stress – effects which will continue into the future as the effects of this Data Breach will continue for years to come.

31. As a result of the Data Breach, Plaintiff anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings this action on behalf of himself and on behalf of the following Class: "All persons whose PII was compromised in the MOVEit data breach" (the "Nationwide Class").

33. Plaintiff also brings this action on behalf of himself and on behalf of the following subclass: "All residents of the State of Connecticut whose PII was compromised in the MOVEit data breach" (the "Connecticut PSC Subclass").

34. Plaintiff also brings this action on behalf of himself and the following subclass: "All persons whose PII was compromised in the MOVEit data breach and obtained from and/or transferred, provided, hosted, or otherwise processes by EY" (the "EY Subclass").

35. Plaintiff also brings this action on behalf of himself and on behalf of the following subclass: "All residents of the State of Connecticut whose PII was compromised in the MOVEit data breach and obtained from and/or transferred, provided, hosted, or otherwise processes by EY" (the "Connecticut EY Subclass").

36. The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

37. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 30,000 members who are geographically dispersed.

38. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members they seek to represent.

39. **Adequacy**: Plaintiff's interests are aligned with the Class they seek to represent, and Plaintiff have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and their counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

40. **Superiority**: A class action is the superior – and only realistic – mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents the potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, because of the complex legal and factual issues of the case. 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.

41. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;

c. Whether Defendants breached their duties to protect Plaintiff's and Class Members' PII;

d. Whether Defendants violated the statutes alleged herein;

e. Whether Plaintiff and all other Class Members are entitled to damages and the measure of such damages and relief.

42. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

43. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

44. Defendants knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

45. This duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Defendants' duties further included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

46. Defendants owed a duty 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, policies, and procedures, and the personnel responsible for them, adequately protected the PII.

47. Specifically, these duties owed by Defendants included the obligation to properly review, assess, and manage the cybersecurity risk posed by third-party vendors and service providers.

48. Defendants owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from their failure to safeguard the PII.

49. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those individuals who entrusted them with their PII, which is recognized by laws and regulations as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

50. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the FTCA, 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.

51. Under the FTCA, Defendants had a duty to employ reasonable security measures. Specifically, this statute 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. 15 U.S.C. § 45.

52. Moreover, Plaintiff and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that – because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices – caused the very same injuries that Defendants inflicted upon Plaintiff and Class Members.

53. Defendants' duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect PII that they acquire, maintain, or store.

54. Defendants owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

55. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendants actively sought and obtained the PII of Plaintiff and Class Members.

56. Defendants breached their duties, and were thus negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. But for Defendants' negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendants include, but are not limited to:

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

b. Failing to comply with – and thus violating – FTCA and its regulations;

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

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

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

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

57. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII, as alleged and discussed above.

58. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Plaintiff and Class Members.

59. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

60. 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.

61. The imposition of a duty of care on Defendants to safeguard the PII they maintained is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

62. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained damages including: (i) invasion of privacy; (ii) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out-of-pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails;

(vii) lost value of their PII; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their PII, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

64. Defendants' negligent conduct is ongoing, in that they still hold the PII of Plaintiff and Class Members in an unsafe and unsecure manner.

65. 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.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Brought on Behalf of the EY Subclass Against BOA)

66. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

67. BOA solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of BOA's regular business practices.

68. Plaintiff and Class Members were required to, and did, provide their PII to BOA in exchange for the use of BOA's banking services.

69. The mutual understanding and intent of Plaintiff and Class Members on one hand, and BOA on the other, is demonstrated by their conduct and course of dealing. BOA required

Plaintiff and Class Members to provide their PII as a condition of using BOA's banking services. Plaintiff and Class Members accepted this offer for services and complied.

70. BOA relied on Plaintiff and Class Members for their business and conferred direct and indirect monetary benefits from the PII provided by Plaintiff and Class Members and thus from Plaintiff and Class Members themselves and had full knowledge of the benefits they conferred.

71. In providing their PII to BOA in exchange for the use of BOA's banking services, and BOA accepting that PII, directly or indirectly, Plaintiff and Class Members conferred a direct benefit on BOA, and entered into implied contracts with BOA by which BOA agreed to keep such information secure and confidential, ensure protection of their PII from unauthorized access or disclosure, and to timely and adequately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

72. Such contracts were made expressly for the benefit of Plaintiff and the Class Members, as it was their PII that BOA agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

73. In entering into these implied contracts, Plaintiff and Class members reasonably believed and expected that BOA's data security practices complied with relevant laws and regulations and were consistent with industry standards, and that BOA would thoroughly vet and select vendors that adequately protect PII.

74. Plaintiff and Class Members would not have entrusted their PII to BOA in the absence of implied contracts between themselves and BOA, under which BOA would keep, and

require the third-party vendors it selects to store, transfer, and process PII in fair, secure, reasonable, and legally complaint ways.

75. Implicit in these agreements between Plaintiff and Class Members and BOA was BOA's obligations to: (i) take reasonable steps to safeguard Plaintiff's and Class Members' PII, including through proper vetting of third party vendors to whom that PII is provided; (ii) prevent unauthorized disclosure of their PII; (c) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (d) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain PII only under conditions that kept such information secure and confidential.

76. BOA knew or should have known that if it were to breach these contracts, Plaintiff and Class Members would be harmed.

77. BOA breached its contracts by, among other things, failing to adequately secure Plaintiff's and Class Members' PII; entrusting the PII to a vendor that fails to safeguard PII; and failing to provide timely notice to Plaintiff and Class Members that their PII was compromised as a result of the Data Breach so that they could take prompt and adequate precautions to mitigate the risks caused by the Data Breach.

78. Plaintiff and Class Members therefore did not receive the benefit of their bargains because they provided their PII to BOA in exchange for an implied agreement by BOA to keep it safe and secure within its computer systems and network environment.

79. BOA's conduct and lax security unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

80. As a direct and proximate result of BOA's breach, Plaintiff and Class Members are at a current and ongoing substantial risk of fraud and identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) lost value of their PII; (vii) future costs of identity theft monitoring; (viii) loss benefit of the bargain and overpaying BOA's services; and (ix) the continued risk to their PII, which remains BOA's control, and which is subject to further breaches, so long as BOA fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

81. As a direct and proximate result of BOA's breach, Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

82. Plaintiff and Class Members are also entitled to injunctive relief requiring BOA to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID protection and credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of the EY Subclass Against EY)

83. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

84. Upon information and belief, EY entered into contracts with BOA to provide consulting services. As part of the provision of these consulting services, BOA entrusted the PII of its customers, which had been directly entrusted to it, to EY.

85. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that EY agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

86. EY knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

87. EY breached its contracts with customers by, among other things, failing to adequately vet its third-party service providers and implement adequate data security measures, and, as a result, Plaintiff and Class Members were harmed by EY's failure to secure their PII.

88. As a direct and proximate result of EY's breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) lost value of their PII; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their PII, which remains in EY's control, and which is subject to further breaches, so long as EY fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

90. Plaintiff and Class Members are also entitled to injunctive relief requiring EY to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID protection and credit monitoring to all Class Members.

FOURTH CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of the Nationwide Class Against PSC)

91. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

92. Upon information and belief, PSC entered into contracts with its government and/or corporate customers to provide secure file transfer services that included data security practices, procedures, designs, and protocols sufficient to safeguard the PII that was entrusted to it.

93. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PII that PSC agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

94. PSC knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

95. PSC breached its contracts with customers by, among other things, failing to adequately secure Plaintiff's and Class Members' PII, and, as a result, Plaintiff and Class Members were harmed by PSC's failure to secure their PII.

96. As a direct and proximate result of PSC's breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) lost value of their PII; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their PII, which remains in PSC's control, and which is subject to further breaches, so long as PSC fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

98. Plaintiff and Class Members are also entitled to injunctive relief requiring PSC to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID protection and credit monitoring to all Class Members.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

99. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

100. Plaintiff and Class Members conferred a monetary benefit on Defendants by providing Defendants with their valuable PII.

101. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII, which cost savings increased the profitability of the services.

102. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

103. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

104. Defendants acquired the monetary benefit and PII, through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

105. Had Plaintiff and Class Members known that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants. Plaintiff and Class Members have no adequate remedy at law.

106. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

107. Furthermore, as a direct and proximate result of Defendants' unreasonable and inadequate data security practices, Plaintiff and Class Members are at a current and ongoing risk

of identity theft and have sustained incidental and consequential damages, including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) lost value of their PII; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their PII, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

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

110. Moreover, Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

111. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

112. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

113. 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 granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those at issue here, that are tortious and violate the terms of the federal statutes described in this Complaint.

114. 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 Plaintiff's and Class Members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their PII. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

115. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect Plaintiff's and Class Members' PII.

116. Defendants still control the PII of Plaintiff and the Class Members.

117. To Plaintiff's knowledge, Defendants have made no announcement that they have changed their data or security practices relating to the PII.

118. To Plaintiff's knowledge, Defendants have made no announcement or notification that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

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

120. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff 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.

121. 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.

122. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and the Class.

124. Plaintiff and Class Members seek a declaration (i) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security; and (ii) 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. engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

e. conduct regular database scanning and security checks; and

f. routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, PII.

SEVENTH CAUSE OF ACTION
INVASION OF PRIVACY-- INTRUSION UPON SECLUSION
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

125. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

126. Plaintiff and Class Members had a reasonable expectation of privacy in the PII that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

127. Defendants' conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

128. By intentionally and/or knowingly failing to keep Plaintiff's and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

129. Defendants knew that an ordinary person in Plaintiff's and Class Members' position would consider Defendants' intentional actions highly offensive and objectionable.

130. Defendants invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

131. Defendants intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

132. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PII were unduly frustrated and thwarted.

133. Defendants' conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests, causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

134. In failing to protect Plaintiff's and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

135. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of himself and the Class.

EIGHTH CAUSE OF ACTION
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

136. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 40 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

137. Plaintiff and Class Members had a reasonable expectation of privacy in the PII Defendants mishandled.

138. As a result of Defendants' conduct, publicity was given to Plaintiff's and Class Members' PII, which necessarily includes matters concerning their private life such as PII.

139. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' PII to be highly offensive.

140. Plaintiff's and Class Members' PII is not of legitimate public concern and should remain private.

141. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) lost value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

143. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

EIGHTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(Brought on Behalf of the Nationwide Class against PSC and on Behalf of the EY Subclass Against EY and BOA)

144. Plaintiff realleges and incorporates by reference preceding paragraphs 1 through 50 as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

145. Plaintiff and Class Members have an interest, both equitable and legal, in PII conveyed to, collected by, and maintained by Defendants and ultimately accessed or compromised in the Data Breach.

146. Defendants have a special relationship with those whose PII they maintain, like Plaintiff and the Class Members.

147. Because of that special relationship, Defendants were provided with and stored sensitive and valuable PII related to Plaintiff and the Class, which they were required to maintain in confidence.

148. Plaintiff and the Class provided Defendants with their PII under an implied agreement of Defendants to limit the use and disclosure of such PII.

149. Defendants owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

150. Defendants had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII. Plaintiff and Class Members have a privacy interest in their personal medical matters, and Defendants had a duty not to disclose confidential PII.

151. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII of Plaintiff and Class Members.

152. Plaintiff's and the Class's PII is not generally known to the public and is confidential by nature.

153. Plaintiff and Class Members did not consent to nor authorize Defendants to release or disclose their PII to an unknown criminal actor.

154. Defendants breached the duties of confidence they owed to Plaintiff and Class Members when Plaintiff's and the Class's PII was disclosed to unknown criminal hackers.

155. Defendants breached their duties of confidence by failing to safeguard Plaintiff's and Class Members' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PII to a criminal third party.

156. But for Defendants' wrongful breach of their duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PII would not have been compromised.

157. As a direct and proximate result of Defendants' breach of Plaintiff's and the Class's confidences, Plaintiff and Class Members have suffered injuries, including: (i) Loss of their

privacy and confidentiality in their PII; (ii) Costs associated with the detection and prevention of identity theft and unauthorized use of their PII; (iii) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach; (iv) Damages to the value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and (v) Mental anguish accompanying the loss of confidences and disclosure of their confidential and PII.

158. As a direct and proximate result of Defendants' breach of their duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

NINTH CAUSE OF ACTION
MASSACHUSETTS GENERAL LAWS CHAPTER 93A
M.G.L. ch. 93A §§ 2 and 9
(On Behalf of Plaintiff and the Nationwide Class Against PSC)

159. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

160. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

161. Plaintiff alleges that PSC committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

162. PSC knew or should have known of the inherent risks in experiencing a data breach if they failed to maintain adequate systems and processes for keeping Plaintiff's and Class

Members' Private Information safe and secure. Only PSC was in a position to ensure that their systems were sufficient to protect against harms to Plaintiff and the Class resulting from a data security incident such as the Data Breach; instead, PSC failed to implement such safeguards.

163. PSC's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. PSC's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

164. PSC knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PII and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

165. PSC failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff's and Class Members' PII, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiff and Class Members in a timely manner that their PII was accessed in the Data Breach.

166. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

167. As a direct and proximate result of PSC's unfair acts and practices, Plaintiff and Class Members have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or fraudulent use of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of PSC's Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in PSC's possession (and/or to which PSC continues to have access) and is subject to further unauthorized disclosures so long as PSC fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PII.

168. Neither Plaintiff nor the other Class Members contributed to PSC's Data Breach.

169. Plaintiff sent a demand for relief, in writing, to PSC on July 12, 2024. Multiple plaintiffs in consolidated actions have sent[14]—or alleged in their complaints that they would send[15]—similar demand letters as required by M.G.L. c. 93A § 9. Plaintiff has not received a

[14] *See, e.g.*, *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[15] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp*., 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al*., 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al*., 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al*., 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al*., 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al*., 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al*., 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al*., 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al*., 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Co., et al*., 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al*., 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al*., 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al*., 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al*., 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al*. , 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al*., 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp*., 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al*., 23-cv-1913 (D. Md.).

written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiff and the Class.

170. Plaintiff therefore seeks actual, punitive, and statutory damages, as appropriate.

171. Based on the foregoing, Plaintiff and the other members of the Class are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

172. Pursuant to M.G.L. ch. 231, § 6B, Plaintiff and other members of the Class are further entitled to pre-judgment interest as a direct and proximate result of PSC's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Plaintiff and other members of the Class are entitled to interest in an amount according to proof.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as the Class Representatives and undersigned counsel as Class Counsel;

B. Find in favor of Plaintiff and the Class on all counts asserted herein;

C. Award Plaintiff and the Class monetary damages, including actual and statutory, compensatory damages, consequential, nominal, general, and punitive damages, to the maximum extent as allowed by law;

D. Award restitution and all other forms of equitable monetary relief;

E. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the PII of Plaintiff and Class

Members, and from refusing to issue prompt, complete, and accurate disclosure to Plaintiff and Class Members;

F. Award injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, and to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. 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;

ii. 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;

iii. 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;

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

v. 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;

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

vii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. 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;

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 its 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 themselves;

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

xvi. requiring, for a period of 10 years, the appointment of 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;

xvii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xviii. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices.

G. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts;

H. Award a mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons.

I. Order Defendants to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiff and Class Members;

J. Order Defendants to pay the costs in notifying Class Members about the judgment and administering the claims process.

K. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowed by law;

L. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial;

M. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable;

N. Distribute any monies recovered on behalf of Class Members or the general public via fluid recovery or cy pres recovery where necessary and as applicable to prevent Defendants from retaining benefits of their wrongful conduct;

O. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity; and

P. Award such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demand a trial by jury on all issues so triable.

Dated: April 17, 2026

Respectfully submitted,

By: */s/ Daniel J. Kurowski*

Daniel J. Kurowski (*pro hac vice*)
Whitney K. Siehl (*pro hac vice*)
HAGENS BERMAN SOBOL SHAPIRO LLP
455 N. Cityfront Plaza Drive, Suite 2410
Chicago, IL 60611
Tel: (708) 628-4949
Fax: (708) 628-4950
dank@hbsslaw.com
whitneys@hbsslaw.com

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 8th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was filed electronically via the Court's CM/ECF system, which will send notice of the filing to all counsel of record.

Dated: April 17, 2026

/s/ Daniel J. Kurowski
Daniel J. Kurowski