UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

LISA MACGILLIVRAY and DANIEL MACGILLIVRAY, individually and on behalf of all others similarly situated, Plaintiffs, v. NATIONAL ACCOUNT SERVICE COMPANY, LLC, BLUE CROSS AND BLUE SHIELD OF MASSACHUSETTS, INC., PROGRESS SOFTWARE CORPORATION, and IPSWITCH, INC., Defendants.	Case No.

CLASS ACTION COMPLAINT

Plaintiffs Lisa MacGillivray and Daniel MacGillivray ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendants National Account Service Company, LLC ("NASCO"), Blue Cross and Blue Shield of Massachusetts, Inc. ("BCBSMA"), Progress Software Corporation ("Progress"), and Ipswitch, Inc. ("Ipswitch") (together, "Defendants").

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their and approximately 804,862 similarly situated individuals' personally identifiable information ("PII") and personal health information ("PHI"), including but not limited to names, addresses, phone numbers, gender, dates of birth, email address, Social Security numbers, health

insurance number, medical ID numbers, dates of service, treatment/diagnostic codes, account information, medical devices/products purchased, and provider names.

2. NASCO provides healthcare technology solutions to Blue Cross and Blue Shield insurance companies, including BCBSMA, a non-profit Massachusetts health insurance provider. Plaintiffs and Class members are customers of insurance companies serviced by NASCO whose PII/PHI was disclosed to unauthorized third parties during a massive data breach compromising Defendants Ipswitch and Progress's MOVEit Transfer and MOVEit Cloud ("MOVEit") software that occurred between approximately May 27, 2023 and May 31, 2023 (the "Data Breach").

3. During the Data Breach, and due to Defendants' data security and privacy shortcomings, unauthorized persons were able to gain access to files containing the PII/PHI of Plaintiffs and Class members by exploiting a vulnerability in the MOVEit platform.

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/PHI 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/PHI from unauthorized access and disclosure.

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

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, breach of implied contract, breach of fiduciary duty, and unjust enrichment, and seek

declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Lisa MacGillivray

7. Plaintiff Lisa MacGillivray ("Plaintiff L. MacGillivray") is a citizen of the Commonwealth of Massachusetts.

8. Plaintiff L. MacGillivray was required to provide her PII/PHI to BCBSMA in connection with obtaining health insurance services or products.

9. Based on representations made by BCBSMA, Plaintiff L. MacGillivray believed that BCBSMA had implemented and maintained reasonable security and practices to protect her PII/PHI, including ensuring that third parties it contracts with and shares PII/PHI with maintain adequate data security and practices.

10. In connection with providing health insurance services or products to Plaintiff L. MacGillivray, BCBSMA collected, maintained, and shared Plaintiff L. MacGillivray's PII/PHI with NASCO. NASCO maintained Plaintiff L. MacGillivray's PII/PHI on its systems, including the MOVEit file-transfer software.

11. Had Plaintiff L. MacGillivray known that Defendants do not adequately protect the PII/PHI in their possession, including BCBSMA by not ensuring that the third parties it contracts with in connection with providing health insurance services or products to its customers maintain adequate data security systems and practices, she would not have agreed to provide her PII/PHI to BCBSMA.

12. Plaintiff L. MacGillivray received a letter from NASCO notifying her that her PII/PHI was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff L. MacGillivray 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/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Plaintiff Daniel MacGillivray

14. Plaintiff Daniel MacGillivray ("Plaintiff D. MacGillivray") is a citizen of the Commonwealth of Massachusetts.

15. Plaintiff D. MacGillivray was required to provide his PII/PHI to BCBSMA in connection with obtaining health insurance services.

16. Based on representations made by BCBSMA, Plaintiff D. MacGillivray believed that BCBSMA had implemented and maintained reasonable security and practices to protect his PII/PHI, including ensuring that third parties it contracts with and shares PII/PHI with maintain adequate data security and practices.

17. In connection with providing health insurance services or products to Plaintiff D. MacGillivray, BCBSMA collected, maintained, and shared Plaintiff D. MacGillivray's PII/PHI with NASCO. NASCO maintained Plaintiff D. MacGillivray's PII/PHI on its systems, including the MOVEit file-transfer software.

18. Had Plaintiff D. MacGillivray known that Defendants do not adequately protect the PII/PHI in their possession, including BCBSMA by not ensuring that the third parties it contracts with in connection with providing health insurance services or products to its customers maintain adequate data security systems and practices, he would not have agreed to provide his PII/PHI to BCBSMA.

19. Plaintiff D. MacGillivray received a letter from NASCO notifying him that his PII/PHI was exposed in the Data Breach.

20. As a direct result of the Data Breach, Plaintiff D. MacGillivray 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/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Defendant National Account Service Company, LLC

21. Defendant National Account Service Company, LLC is a Delaware corporation with its principal place of business located at 1200 Abernathy Rd., Suite 1000, Atlanta, GA 30328. It may be served through its registered agent, C T Corporation System, 289 S. Culver St., Lawrenceville, GA 30046.

Defendant Blue Cross and Blue Shield of Massachusetts, Inc.

22. Defendant Blue Cross and Blue Shield of Massachusetts, Inc., is a Massachusetts corporation with its principal place of business located at 101 Huntington Ave., Suite 1300, Boston, MA 02199. It may be served through its registered agent, Corporation Service Company, 84 State St., Boston, MA 02109.

Defendant Progress Software Corporation

23. Defendant Progress Software Corporation is a Delaware corporation with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, MA 01803.

Defendant Ipswitch, Inc.

24. Defendant Ipswitch, Inc. is a Massachusetts corporation with its principal place of business located at 15 Wayside Road, 4th Floor, Burlington, MA 01803.

JURISDICTION AND VENUE

25. 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. Further, greater than two-thirds of the Class Members reside in states other than the states in which Defendants are citizens.

26. The Court has personal jurisdiction over Defendant National Account Service Company, LLC because Defendant transacts significant business in Massachusetts, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Massachusetts through its promotion, marketing, and sale of healthcare technology services.

27. The Court has personal jurisdiction over Defendant Blue Cross and Blue Shield of Massachusetts, Inc., because it has its principal office in Massachusetts, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Massachusetts through its promotion, marketing, and sale of health insurance services and products.

28. The Court has personal jurisdiction over Defendants Progress Software Corporation, and Ipswitch, Inc. because Defendants have their principal offices in Massachusetts, and otherwise have sufficient minimum contacts with and intentionally avail themselves of the markets in Massachusetts through their promotion, marketing, and sale of the MOVEit software and other software, products, and related services.

29. Venue properly lies in this judicial district because, *inter alia,* BCBSMA's, Progress's, and Ipswitch's principal place of business are located in this District, Defendants transact substantial business in this District, and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Ipswitch, Inc., Progress Software, and the Unsecure MOVEit Software

30. Ipswitch is an IT software development company founded in 1991 in Burlington, Massachusetts. Ipswitch sells its software and related products and services, including MOVEit solutions, directly and through resellers and distributors in the United States.

31. Progress, a public domestic software company based in Massachusetts, acquired Ipswitch in May 2019 for approximately $225 million.

32. Ipswitch developed and through Progress sells the MOVEit software, which they claim is "the leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities."[1]

33. On their websites, Defendants Ipswitch and Progress make a host of claims about data security and their MOVEit product. Ipswitch claims, generally, that its "Enterprise File Transfer Solutions – Mak[e] the networked world a safer place."[2] Its website states: "Our efficient, easy-to-use products empower customers to respond faster to business demands through accelerated implementation and improved productivity and security."[3]

34. Specific to MOVEit, Ipswitch claims that "MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems." [4] Ipswitch claims its MOVEit Transfer and MOVEit Cloud products give customers "control" over their businesses;

---

[1] *MOVEit*, IPSWITCH, https://www.ipswitch.com/moveit (last accessed Nov. 9, 2023).

[2] *Ipswitch.com*, IPSWITCH, https://www.ipswitch.com (last accessed Nov. 9, 2023).

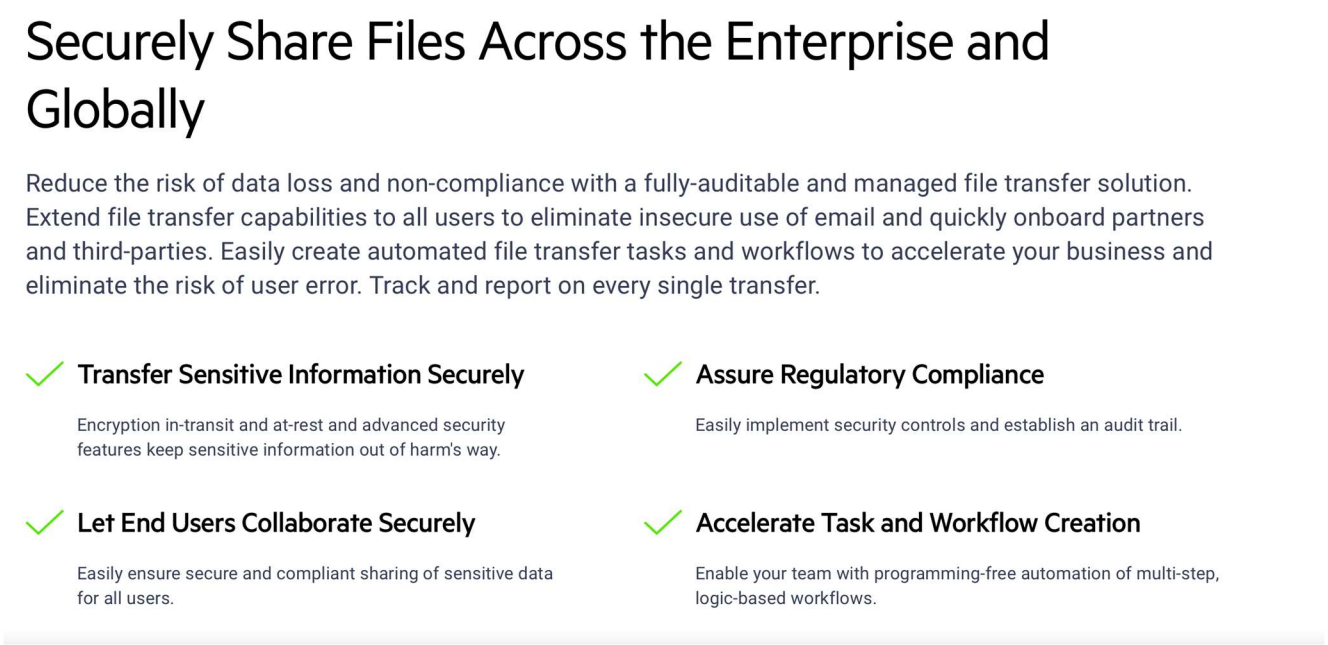
[3] *Id*.

[4] *See MOVEit*, *supra* note 1.

"provides full security, reliability and compliance"; provide "encryption, security, activity tracking tamper-evident logging, and centralized access controls to meet your operational requirements"; "[r]eliably and easily comply with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR"; and provide "secure and managed file transfer."[5]

35. Progress makes similar statements about data security. Its website claims "MOVEit provides secure collaboration and automated file transfers of sensitive data" and that it provides "[e]ncryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[6]

36. Progress also touts all of the following on its website regarding MOVEit:[7]



37. As demonstrated above, Defendants Ipswitch and Progress heavily tout and promote the MOVEit products and services as capable of safely transferring sensitive information.

---

[5] *Id.*

[6] *MOVEit*, PROGRESS, https://www.progress.com/moveit (last accessed Nov. 9, 2023).

[7] *Id.*

Despite these assurances and claims, Defendants Ipswitch and Progress failed to offer safe and secure file transfer products and failed to adequately protect Plaintiffs' and Class members' PII.

38. This is because the products that Defendants Ipswitch and Progress offered, and which NASCO used, were not secure. When the Data Breach occurred, there was a critical vulnerability in the MOVEit software referred to as CVE-2023-34362. Specifically, Defendants Ipswitch and Progress identified that MOVEit's web-based front end is affected by a critical structured query language (SQL) injection vulnerability/attack vector that can be exploited by an unauthenticated attacker to access databases associated with the product.

39. All of the Defendants knew or should have known that MOVEit leaves the PII/PHI of NASCO's clients' customers, including Plaintiffs and Class members, exposed to security threats. Despite this, Ipswitch and Progress continued to offer MOVEit file transfer products without adequately testing and identifying the vulnerabilities in the products, and patching or otherwise eliminating those threats.

40. Similarly, NASCO continued to use the MOVEit software without adequately ensuring it was secure and that Ipswitch and Progress had adequate data security systems and practices in place to protect Plaintiffs' and Class members' PII/PHI. As one cybersecurity company noted, "Just because a piece of software claims to be 'secure' doesn't mean that it is. Customers must always validate that the software they use is secure and is configured in a way that can protect against cyberattacks."[8]

[8] Avishai Avivi, *MOVEIt Vulnerability: A Painful Reminder That Threat Actors Aren't the Only Ones Responsible for a Data Breach*, SAFEBREACH (June 21, 2023), https://www.safebreach.com/moveit-vulnerability-a-painful-reminder-that-threat-actors-arent-the-only-ones-responsible-for-a-data-breach/.

NASCO and BCBSMA

41. NASCO is "a healthcare technology company dedicated to co-creating digital health solutions for Blue Cross and Blue Shield companies,"[9] including BCBSMA. It provides a "robust portfolio of premier healthcare technology solutions designed to enable [Blue Cross and Blue Shield] plan success."[10]

42. BCBSMA is a "community-focused, not-for-profit health plan."[11] It is Massachusetts's largest not-for profit health plan and serves approximately three million members.[12]

43. BCBSMA's website contains a privacy policy called "Commitment to Confidentiality."[13] In the policy BCBSMA states, "We respect your right to privacy."[14] BCBSMA promises it "won't disclose personally identifiable information about you without your permission, unless the disclosure is necessary to provide our services to you or is otherwise in accordance with the law."[15] In the privacy policy, BCBSMA lists the limited ways it may disclose its customers' information without their written consent including, *inter alia*, for treatment, payment, and

[9] *About Us*, NASCO, https://www.nasco.com/about/ (last accessed Nov. 9, 2023).

[10] *Solutions*, NASCO, https://www.nasco.com/solutions-v2/ (last accessed Nov. 9, 2023).

[11] *Our Business Approach*, BCBSMA, https://www.bluecrossma.org/aboutus/financials (last visited Nov. 9, 2023).

[12] *See We're Ready for Anything*, BCBSMA, https://www.bluecrossma.org/aboutus/steadfast-support (last visited Nov. 9, 2023).

[13] *See Commitment to Confidentiality*, BCBSMA, https://www.bluecrossma.org/disclaimer/member-rights-and-responsibilities/commitment-to-confidentiality (last accessed Nov. 9, 2023).

[14] *Id.*

[15] *Id.*

research purposes.[16] BCBSMA promises it "won't use or disclose information about you without your written authorization" other than as described in the privacy policy.[17]

44. BCBSMA acknowledges it is "required by law to protect the confidentiality of information about you and to notify you in case of a breach affecting your information."[18] BCBSMA further admits it "must comply with any state or federal privacy laws" requiring privacy protections.[19]

45. The privacy policy claims BCBSMA uses "use physical, electronic, and procedural safeguards to protect your privacy."[20] It further states BCBSMA shares information "subject to contracts that limit use and disclosure [of personal information] for intended purposes."[21]

46. BCBSMA also acknowledges the existence of "health care fraud," which it notes "is predicted to become even more common in the future, includes everything from health care identity theft to billing for health care services that were never performed."[22] BCBSMA is aware that "[l]osses from health care fraud lead to increased health care costs, which can make care more expensive for all of us."[23]

---

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *See id.*

[20] *Id.*

[21] *Id.*

[22] *Health Care Fraud*, BCBSMA, https://www.bluecrossma.org/disclaimer/member-rights-and-responsibilities/health-care-fraud (last visited Nov. 8, 2023).

[23] *Id.*

47. BCBSMA advises its customers to "never share your personal information unless you are absolutely sure you're [sharing with] someone you can trust."[24] As BCBSMA is aware, after data is shared with a third party, the third party can use that data for any purpose, "including sharing it with additional third parties without your knowledge or consent."[25]

48. NASCO's website claims it ensures security and compliance, "so you can feel confident that your health plan and member data are secure."[26] The website also states, "With a watchful eye on increasing cybersecurity risks, NASCO remains committed to maintaining the highest levels of security and data protection."[27] NASCO promises its "security profile is reviewed annually to assure we continue to maintain the proper controls for protecting customer and member data."[28]

49. BCBSMA shared Plaintiffs' and Class members' PII/PHI with NASCO, which in turn shared that information with Progress and Ipswitch through its use of the MOVEit software in connection with providing health insurance services or products to Plaintiffs and Class members.[29] In doing so, NASCO and BCBSMA failed to ensure that Ipswitch and Progress

---

[24] *Id.*

[25] *Allowing Access to Your Private Health Information*, BCBSMA, https://www.bluecrossma.org/disclaimer/allowing-access-to-your-private-health-information (last accessed Nov. 9, 2023).

[26] *E.g.*, *Servicing & Advocacy*, NASCO, https://www.nasco.com/servicing-and-advocacy/ (last accessed Nov. 9, 2023).

[27] *NASCO's Commitment to Security and Data Protection*, NASCO (Oct. 17, 2022), https://www.nasco.com/nascos-commitment-to-security-and-data-protection/ (last accessed Nov. 9, 2023).

[28] *Id.*

[29] *See Notice Letter*, available at *NASCO Data Breach Notification*, OFF. OF THE ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/9925f2a7-566b-45bb-8b25-cb67ddfb9967.shtml (under "Notification and Protection Services" heading, click linked titled "NASCO - Individual Notification Letter Sample.pdf").

implemented and maintained adequate data security practices to protect Plaintiffs' and Class member's PII/PHI from unauthorized access, disclosure, and theft

The Data Breach

50. On or about May 30, 2023, unauthorized persons exploited a vulnerability in the MOVEit software to acquire files containing the sensitive PII/PHI of Plaintiffs and Class members.[30]

51. According to reports, the Clop (also known as CLOP or Cl0p) ransomware gang is responsible for the attack on the MOVEit platform.[31]

52. NASCO claims it learned of the Data Breach on July 12, 2023.[32] Despite this, NASCO waited until approximately October 27, 2023, over three months later, to begin notifying its customers of the Data Breach.[33]

53. The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI first warned on June 7, 2023, that the Clop ransomware gang was exploiting a vulnerability in MOVEit Transfer. "Internet-facing MOVEit Transfer web applications were infected with a specific malware used by CL0P, which was then used to steal data from underlying MOVEit Transfer databases," the advisory said, as it explained how threat actors carried out the attack.[34]

---

[30] *See id.*

[31] *See Clop Gang to Earn Over $75 Million from MOVEit Extortion Attacks*, BLEEPING COMPUTER (July 21, 2023, 12:34 PM), https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/.

[32] *Notice Letter*, *supra* note 29.

[33] *See NASCO Provides Notification and Support Related to Data Security Incident*, PR NEWSWIRE (Oct. 27, 2023 5:00 PM), https://www.prnewswire.com/news-releases/nasco-provides-notification-and-support-related-to-data-security-incident-301970341.html.

[34] Bruce Sussman, *Clop Ransomware and the MOVEit Cyberattack: What to Know*, BLACKBERRY BLOG (June 19, 2023), https://blogs.blackberry.com/en/2023/06/clop-ransomware-and-moveit-cyberattack.

54. A senior CISA officer informed reporters that "several hundred" businesses and organizations in the United States may be impacted by the hacking campaign in addition to government entities.[35]

55. Plaintiffs and Class members' sensitive PII/PHI was compromised in the Data Breach as a result of Ipswitch and Progress's unsecure MOVEit file transfer product being exploited by cyber criminals, and because BCSBA and NASCO failed to ensure the third parties they contract with to provide services to Plaintiffs and Class members maintained adequate data security systems and practices.

Defendants Knew that Criminals Target PII

56. At all relevant times, Defendants knew, or should have known, that the information 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/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

57. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata

[35] Onur Demirkol, *US Government Under Seige: MOVEit Breach Exposes Critical Data to Ruthless Clop Ransomware Attack*, DATACONOMY (June 19, 2023), https://dataconomy.com/2023/06/19/moveit-breach-data-clop-ransomware/ (last accessed Nov. 9, 2023).

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."[36]

58. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[37] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[38]

59. PII/PHI is a valuable property right.[39] The value of PII/PHI as a commodity is measurable.[40] "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."[41] American companies are estimated to have spent over $19 billion on acquiring

---

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

[37] *See 2023 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed Nov. 9, 2023).

[38] *See id*.

[39] *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.

[40] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[41] 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.

personal data of consumers in 2018.[42] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

60. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, 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.

61. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[43] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[44]

62. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[45] According to a report released by the Federal Bureau of Investigation's

---

[42] 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/.

[43] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[44] *Id.*

[45] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[46]

63. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[47] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[48]

64. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[49]

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

---

[46] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[47] Steager, *supra* note 43.

[48] *Id.*

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

Theft of PII Has Grave and Lasting Consequences for Victims

66. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[50] [51]

67. 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 permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[52]

68. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[53]

---

[50] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 9, 2023).

[51] 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).

[52] *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/.

[53] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Nov. 9, 2023).

69. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[54] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[55] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [56] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[57]

70. 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.

71. 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

---

[54] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[55] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 46.

[56] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 9, 2023).

[57] *Id*.

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."[58]

72. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [59]

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

[59] *See* Dixon & Emerson, *supra* note 54.

73. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person 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 individuals up to three years to learn that information.[60]

74. It is within this context that 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 Class Members

75. Plaintiffs and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' 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/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

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

---

[60] 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.

77. Plaintiffs bring this action on their own behalf, and on behalf of the following Class of similarly situated persons:

> All United States residents whose personally identifiable information or personal health information was in the possession of NASCO and was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

78. Excluded from the Class are: (i) Defendant Ipswitch, Inc. and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; (ii) Defendant Progress Software Corporation and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; (iii) Defendant Blue Cross and Blue Shield of Massachusetts, Inc., and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; (iv) Defendant National Account Service Company, LLC, and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; and (v) the judge(s) presiding over this matter and the clerks of said judge(s).

79. 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.

80. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. NASCO reported to the Maine Attorney General that the Data Breach affected 804,862 of its clients' customers.[61]

[61] *NASCO Data Breach Notification*, OFF. OF THE ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/9925f2a7-566b-45bb-8b25-cb67ddfb9967.shtml (last accessed Nov. 9, 2023).

81. 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/PHI from unauthorized access and disclosure, including ensuring that the third parties it contracts with to provide services had adequate data security measures in place;

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

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/PHI from unauthorized access and disclosure;

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

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

82. 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.

83. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI 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.

84. 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.

85. 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

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

87. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in their possession, custody, or control.

88. Defendants' duties arise from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164,

Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"). Plaintiffs and Class members are the persons that the HIPPA Privacy and Security Rules were intended to protect and the harm that Plaintiffs and Class members suffered is the type of harm the rules were intended to guard against.

89. Defendants' duties also 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/PHI. Plaintiffs and Class members are the persons that Section 5 of the FTCA was intended to protect and the harm that Plaintiffs and Class members suffered is the type of harm Section 5 of the FTCA intended to guard against.

90. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and Class members' PII/PHI and the importance of maintaining secure systems, including ensuring third party vendors employed adequate data security practices. Defendants knew or should have known that they faced an increased threat of customer data theft, as judged by the many data breaches that have targeted companies that stored PII/PHI in recent years.

91. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they collect, store, and maintain, and the resources at their disposal, Defendants should have taken care to identify the vulnerabilities to their systems or to their third-party vendors' systems and prevented the Data Breach from occurring.

92. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI 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/PHI entrusted to them—including Plaintiffs' and Class members' PII/PHI.

93. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI 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/PHI to unauthorized individuals.

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

95. 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 suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' 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/PHI compromised as a result of the Data Breach; (vii) loss of value of the PII/PHI that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
Against BCBSMA Only

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

97. Plaintiffs bring this claim only against BCBSMA.

98. In connection with the dealings Plaintiffs and Class members had with Defendants, Plaintiffs and Class members entered into implied contracts with BCBSMA.

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

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

101. Had Plaintiffs and Class members known that BCBSMA would not adequately protect its customers' and former customers' PII/PHI, they would not have provided BCBSMA with their PII/PHI.

102. Plaintiffs and Class members performed their obligations under the implied contracts when they provided BCBSMA with their PII/PHI, either directly or indirectly.

103. BCBSMA breached its obligations under its implied contracts with Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards, including by not ensuring that the third parties it contracts with and shares PII/PHI with implemented and maintained adequate security protocols and procedures.

104. BCBSMA's breach of its obligations of the implied contracts with Plaintiffs and Class members directly resulted in their PII/PHI being exposed in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered as a result of and in connection thereto.

105. Plaintiffs and all other Class members were damaged by BCBSMA'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/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, 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 III
BREACH OF FIDUCIARY DUTY
Against BCBSMA Only

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

107. Plaintiffs bring this claim only against BCBSMA.

108. Plaintiffs and Class members gave BCBSMA their PII/PHI in confidence, believing that BCBSMA would protect that information. Plaintiffs and Class members would not have provided BCBSMA with this information had they known it would not be adequately protected.

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

110. Due to the nature of the relationship between BCBSMA and Plaintiffs and Class members, Plaintiffs and Class members were entirely reliant upon BCBSMA to ensure that their PII/PHI was adequately protected. Plaintiffs and Class members had no way of verifying or influencing the nature and extent of BCBSMA's data security policies and practices or the extent to which it ensured that the third parties it contracts with and shares PII/PHI with maintained adequate data security practices and protocols, and BCBSMA was in an exclusive position to guard against the Data Breach.

111. BCBSMA 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 safeguard Plaintiffs' and Class members' PII/PHI that it collected, failing to ensure Plaintiffs' and Class members' PII/PHI was shared with entities with adequate data

protection systems and measures in place, and failing to notify Plaintiffs and Class members of the Data Breach in a timely manner.

112. As a direct and proximate result of BCBSMA'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/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' 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/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

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

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

115. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of their valuable PII/PHI and through money paid for services, a portion of which Plaintiffs and Class members reasonably expected would be used to protect their PII/PHI.

116. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class members by storing or transferring the PII/PHI, or otherwise using it to facilitate their business, and providing services to Plaintiffs and Class members.

117. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the loss of value of Plaintiffs' and Class members' PII/PHI. Plaintiffs and Class members also 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.

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

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, by and through undersigned counsel, 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 Plaintiffs as class representative and undersigned counsel as class counsel;

B. Award Plaintiffs and Class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

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

E. Award Plaintiffs and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

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

Dated: November 10, 2023

Respectfully submitted,

/s/ David Pastor
David Pastor (BBO 391000)
PASTOR LAW OFFICE PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617-742-9700
Fax: 617-742-9701
Email: dpastor@pastorlawoffice.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
Email: b.barnow@barnowlaw.com
Email: aparkhill@barnowlaw.com

Attorneys for Plaintiffs and the Proposed Class

* *pro hac vice forthcoming*

ClassAction.org
