UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CHRISTOPHER PIPES, individually and on behalf of all others similarly situated, Plaintiffs, v. IPSWITCH, INC. and PROGRESS SOFTWARE CORPORATION, Defendants.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Christopher Pipes ("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, by and through undersigned counsel, brings this Class Action Complaint against Defendants Ipswitch, Inc. and Progress Software Corporation (together, "Defendants").

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of himself and all other individuals ("Class Members") who had their sensitive personal information—i.e., information that is or could be used, whether on its own or in combination with other information, to identify, locate, or contact a person, including, without limitation: names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers ("SSN"), drivers' license information, tax records, bank account and routing information, and other personally identifying information ("Personal Information")—disclosed to unauthorized third parties during a massive data breach compromising Defendants' MOVEit Transfer and MOVEit Cloud ("MOVEit") software that occurred on or about May 27, 2023 (the "Data Breach").

2. MOVEit is an industry-leading third-party data transfer service used to send large files. It is widely used across the country and around the world. Reports are rapidly emerging of newly discovered exposures of sensitive data in this major international cyber-attack.

3. During the Data Breach, and due to Defendants' data security and privacy shortcomings, unauthorized persons were able to gain access to Defendants' clients' files by exploiting a vulnerability in the MOVEit platform. Specifically, the attacks, which appear to be ongoing, reportedly have been conducted by a ransomware gang, which began hacks of MOVEit transfer servers on May 27, 2023, using a vulnerability tracked as CVE-2023-34362.

4. The MOVEit attacks have resulted in widespread disclosures of data breaches domestically and worldwide, impacting various companies, federal government agencies, and local state agencies. Numerous impacted companies have announced being impacted by the MOVEit Data Breach, while others will continue to disclose breaches in the near term.

5. Plaintiff is a victim of Defendants' conduct and the MOVEit Data Breach. On June 15, 2023, the Louisiana Office of Motor Vehicles ("OMV") issued a press release confirming that it is one of the still undetermined number of government entities, businesses, and other organizations impacted by the MOVEit Data Breach. OMV confirmed that it believes all Louisianans with a state-issued driver's license, ID, or car registration likely had the following data exposed to the cyber attackers: name, address, Social Security number, birthdate, height, eye color, driver's license number, vehicle registration number, and handicap placard information. According to reports, about 6 million Louisiana OMV records were impacted by the breach.

6. Plaintiff, a Louisiana citizen, had his Personal Information disclosed as a result of the Louisiana OMV episode of the MOVEit Data Breach. Plaintiff and millions of other Class Members

have had their data privacy, data security, and identities exposed to cybercriminals and their Personal Information jeopardized because of the Data Breach.

7. Defendants are and at all relevant times were well aware of the data security shortcomings in their MOVEit file transfer software. Indeed, software vulnerabilities have become ubiquitous in large data breaches. Nevertheless, Defendants failed to take steps to undertake the necessary testing for and eliminate the vulnerabilities in the MOVEit software, putting its file transfer service clients and their clients' customers, employees, and other affiliated persons at risk of being impacted by a breach.

8. Defendants' failure to ensure that its MOVEit file transfer software and services were adequately secure fell far short of its obligations and Plaintiff's and Class Members' reasonable expectations for data privacy, has jeopardized the security of their Personal Information, and has put them at a serious and continuing risk of fraud and identity theft.

9. As a result of Defendants' conduct and the Data Breach, Plaintiff's and Class Members' privacy has been invaded. Their Personal Information is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

10. Plaintiff Christopher Pipes is a citizen of Louisiana and resides in Calhoun, Louisiana. Plaintiff is a holder of a state-issued Louisiana driver's license and thus was a victim of the OMV episode of the MOVEit Data Breach. As a result of and following the Data Breach, Plaintiff Pipes spent approximately 3 hours setting up credit freezes with the major credit bureaus and checking his Credit Karma and bank accounts for signs of fraudulent activity. Plaintiff estimates he

will continue to spend approximately one hour per week on breach mitigation efforts and monitoring for fraud.

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

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

JURISDICTION AND VENUE

13. 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 ($5,000,000.00) and is a class action in which Plaintiff is a citizen of a state different from Defendants. Further, greater than two-thirds of the Class Members reside in states other than the state in which Defendants are citizens.

14. The Court has personal jurisdiction over Defendants because Defendants have their principal office in Massachusetts; transact significant business 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 MOVEit software and other software, products, and related services.

15. Venue properly lies in this judicial district because, *inter alia,* Defendants have their principal places of business, transact substantial business, have agents, and are otherwise located in this District; and a substantial part of the conduct giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

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

16. Defendant Ipswitch, Inc. ("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.

17. Ipswitch is now a part of Defendant Progress Software Corporation ("Progress"), a public domestic software company based in Massachusetts. Progress acquired Ipswitch in May 2019 for approximately $225 million.

18. Ipswitch developed and through Progress sells MOVEit, which Defendants 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]

19. On their websites, Defendants 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]

20. 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

[1] *MOVEit*, IPSWITCH, https://www.ipswitch.com/moveit (last accessed June 20, 2023).

[2] *Ipswitch.com*, IPSWITCH, https://www.ipswitch.com (last accessed June 20, 2023).

[3] *Id*.

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; "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]

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

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

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

[5] *Id*.

[6] *MOVEit*, PROGRESS, https://www.progress.com/moveit (last accessed June 20, 2023).

[7] *Id*.

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

24. Despite these assurances and claims, Defendants failed to offer safe and secure file transfer products and failed to adequately protect Plaintiff's and Class Members' Personal Information involved in its clients' use of Defendants' MOVEit products.

25. This is because the products that Defendants offered, and which their clients used, were not secure.

26. Despite knowing or that Defendants should have known, that MOVEit leaves Defendants' customers and the third parties interacting and transacting with their file transfer customers (like Plaintiff and other Class Members) exposed to security threats, they continued to offer and transact business with their customers using the MOVEit file transfer products without adequately testing and identifying the vulnerabilities in the products, and patching or otherwise eliminating those threats.

B. The MOVEit Data Breach

27. On May 31, 2023, Progress and Ipswitch alerted their customers about a critical vulnerability in the MOVEit software referred to as CVE-2023-34362. Specifically, Defendants 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.

28. According to reports, the Clop (also known as CLOP or Cl0p) ransomware gang is responsible for the attack on the MOVEit platform, which has led to compromised networks around the globe, including across the United States.

29. 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.[8]

30. 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.[9]

31. The list of impacted entities and organizations that are MOVEit customers continues to grow, but reports indicate that the following domestic entities have indicated potential impact or confirmed impact by the MOVEit breach, among others ("Impacted MOVEit Clients"):

- Louisiana Office of Motor Vehicles;
- Oregon Department of Motor Vehicles;
- Oak Ridge Associated Universities (U.S. Department of Energy);
- Waste Isolation Pilot Plant (U.S. Department of Energy);
- Umpqua Bank;
- UnitedHealthcare Student Resources;
- Leggett & Platt;
- University System of Georgia;
- 1st Source;
- First National Bankers Bank;
- Putnam Investments
- Datasite;
- National Student Clearinghouse;
- Gen Digital.

[8] 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.

[9] Onur Demirkol, *US Government Under Seige: MOVEit Breach Exposes Critical Data to Ruthless Clop Ransomware Attack*, DATA CONOMY (June 19, 2023), https://dataconomy.com/2023/06/19/moveit-breach-data-clop-ransomware/ (last accessed June 20, 2023).

C. Impact of the Data Breach

32. As a result of the MOVEit Data Breach, Plaintiff and many millions of individuals have had their sensitive Personal Information exposed as a result of Defendants' unsecure MOVEit file transfer product being exploited by cyber criminals during the Data Breach.

33. The harm caused to Plaintiff and Class Members by the Data Breach is already apparent. Criminal hacker groups have made ransomware payment demands upon Impacted MOVEit Clients and have already publicly disseminated information about the Data Breach[10] and, potentially, lists containing sensitive Personal Information, presumably for those MOVEit customers who decline to pay the ransom demand.

34. Even if Impacted MOVEit Clients pay the ransom, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

35. The breach creates a heightened security concern for Plaintiff and Class Members because SSNs and other sensitive information was or may be among the data exposed during the Data Breach.

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

---

[10] Carly Page, *Ransomware Gang Lists First Victims of MOVEit Mass-Hacks, Including US Banks and Universities*, TechCrunch (June 15, 2023, 4:45 AM CDT), https://techcrunch.com/2023/06/15/moveit-clop-mass-hacks-banks-universities/.

37. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[11]

38. Defendants had a duty to keep sensitive information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to the Louisiana OMV and other Impacted MOVEit Clients with the common sense understanding any business partners to which these entities disclosed Personal Information (i.e., Defendants) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

39. Defendants' data security obligations were particularly important given the substantial increase in data breaches—particularly those involving SSNs—in recent years, which are widely known to the public and to anyone in Defendants' industry of data collection and transfer.

40. Data breaches are by no means new, and they should not be unexpected. These types of attacks should be anticipated by companies that collect and store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks. Defendants cannot feign ignorance. Their representations about MOVEit acknowledge the need and importance for "compliance with regulations such as PCI, HIPAA and GDPR" in collecting, storing, and transferring sensitive data.

---

[11] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

41. It is well known among companies that store sensitive personally identifying information that sensitive information—like SSNs—is valuable and frequently targeted by criminals. *Business Insider* has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[12]

42. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

43. There may be a time lag between when sensitive Personal Information is stolen and when it is used. For example, 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.[13]

44. With access to an individual's sensitive Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: opening utility accounts using the victim's identity; file a fraudulent tax return using the victim's information; or even give the victim's personal information to police during an arrest.[14]

45. Sensitive Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web

---

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

[13] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[14] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 20, 2023).

for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other sensitive Personal Information directly on various illegal websites making the information publicly available, often for a price.

46. Personal Information is a valuable property right.[15] The value of Personal Information as a commodity is measurable.[16] "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."[17] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[18]

47. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect MOVEit, which it should have known was unsecure, from being breached, leaving its clients (including the Impacted MOVEit Clients) and all persons who provide sensitive Personal Information to those clients (i.e., Plaintiff and the Class Members) exposed to risk of fraud and identity theft.

---

[15] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. 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.

[16] *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.

[17] 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.

[18] *See* 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/.

48. Defendants are, and at all relevant times have been, aware that the sensitive Personal Information they handle and store in connection with providing their file transfer services is highly sensitive. As companies that provide file transfer services involving highly sensitive information, Defendants are aware of the importance of safeguarding that information and protecting their systems and products from security vulnerabilities, and Defendants repeatedly acknowledge the importance of data security and compliance with data privacy requirements and regulations on their websites for MOVEit.

49. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and were alerted to the risks associated with failing to ensure that their file transfer product MOVEit was adequately secured.

50. Despite the well-known risks of hackers, cybercriminals, data breaches, and cybersecurity intrusions, Defendants failed to employ adequate data security measures in connection with offering its MOVEit file sharing software products and related services in a meaningful way in order prevent breaches, including the Data Breach.

51. The security flaws inherent to MOVEit run afoul of industry best practices and standards. Had Defendants adequately tested MOVEit for security flaws and vulnerabilities, and undertaken industry best practices and steps to protect and secure MOVEit, they could have prevented the Data Breach.

52. Despite the fact that Defendants were on notice of the very real possibility of data theft and data breaches associated with the MOVEit products, they failed to make necessary changes to the product or to stop offering it while working these issues out and permitted a massive intrusion to occur that resulted in disclosure of Plaintiff's and Class Members' Personal Information to criminals.

53. Defendants allowed Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

54. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has commented that "[i]f your data was stolen through a data breach that means you were somewhere out of compliance . . . ."[19]

55. As a result of the events detailed herein, Plaintiff 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 Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (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 Personal Information 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 Personal Information compromised as a result of the Data Breach; (vii) loss of value of the Personal Information that was compromised in the Data Breach; (viii) overpayment for the services that were received without adequate data security; and (ix) loss of privacy.

56. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach, i.e., through ransom demands and as evidenced by news that Impacted MOVEit Client information is being posted on Clop's website.

[19] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

57. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they have experienced fraud and/or face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

58. Plaintiff brings this action on his own behalf, and on behalf of the following Class:

> All natural persons who are residents of the United States whose Personal Information was compromised in the MOVEit Data Breach, including all natural persons who were sent a notice indicating that their Personal Information may have been compromised in the MOVEit Data Breach (the "Nationwide Class").

59. Excluded from the Class are: (i) Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns; and (ii) any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

60. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many millions of members who are geographically dispersed.

61. **Typicality**: Plaintiff and all Class Members were injured through Defendants' uniform misconduct and assert similar claims against Defendants. Accordingly, Plaintiff's claims are typical of Class Members' claims.

62. **Adequacy**: Plaintiff's interests are aligned with the Class he seeks to represent, and he has retained counsel with significant experience prosecuting complex class action cases, including cases involving privacy and data security violations. Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and Plaintiff's counsel.

63. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Member's 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 a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by 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.

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

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants were negligent;
- whether Defendants' data security practices and the vulnerabilities of its MOVEit file transfer products/software resulted in the unauthorized disclosure of Plaintiff's and other Class Members' Personal Information;
- whether Defendants violated privacy rights and invaded Plaintiff's and Class Members' privacy; and
- whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

65. Given that Defendants have engaged in a common course of conduct as to Plaintiff

and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

67. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting their Personal Information in their possession, custody, or control.

68. Defendants' duties arise from, *inter alia*, 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 business, 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.

69. Defendants knew the risks of collecting and storing Plaintiff's and Class Members' Personal Information and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted companies that stored Personal Information in recent years.

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

71. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Personal Information entrusted to it—including Plaintiff's and Class Members' Personal Information.

72. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems resulting in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Personal Information to unauthorized individuals.

73. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

74. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff 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 Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (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 Personal Information 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 Personal Information compromised as a result of the Data Breach; (vii) loss of value of the Personal Information that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
UNJUST ENRICHMENT

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

76. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of their valuable Personal Information.

77. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members by storing or transferring the Personal Information.

78. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the loss of value of Plaintiff's and Class Members' Personal Information.

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

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

PRAYER FOR RELIEF

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

B. Award Plaintiff 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 Plaintiff and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

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

JURY TRIAL DEMANDED

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

Dated: June 21, 2023

Respectfully submitted,

/s/ David Pastor

DAVID PASTOR (BBO 391000)
dpastor@pastorlawoffice.com
PASTOR LAW OFFICE PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617.742.9700
Fax: 617.742.9701

ANDREW W. FERICH (*pro hac vice* to be filed)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

TINA WOLFSON (*pro hac vice* to be filed)
twolfson@ahdootwolfson.com
DEBORAH DE VILLA (*pro hac vice* to be filed)
ddevilla@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW (*pro hac vice* to be filed)
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL (pro hac vice to be filed)
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312-621-2000
Facsimile: 312-641-5504

Attorneys for Plaintiff and the Proposed Class