Leanna A. Loginov (NJ Bar No. 389742022)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
E: lloginov@shamisgentile.com

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

PEGGY BORDELON, individually and on behalf of all others similarly situated, Plaintiff, v. **CONDUENT BUSINESS SERVICES, LLC,** Defendant.	Case No. **COMPLAINT AND DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Peggy Bordelon ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant, Conduent Business Services, LLC ("Conduent" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, and upon information and belief and her counsel's investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks injunctive and declaratory relief arising from Defendant's failure to safeguard the names ("Personally Identifiable Information")[1] and treatment cost information, treatment date information, and health insurance numbers ("Protected Health Information") (together, "Private Information") of Plaintiff and Class members which resulted in unauthorized access to its information systems from October 21, 2024 to January 13, 2025, and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant, Conduent Business Services, LLC provides digital business solutions and services to clients across the commercial, government, and transportation sectors, with its principle place of business in Florham Park, New Jersey[2].

3. As explained in detail herein, on or about January 13, 2025, Conduent detected unusual activity in its computer systems and ultimately determined that an

[1] The Federal Trade Commission ("FTC") defines "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." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

[2] https://www.conduent.com/about-conduent/?_gl=1*9qou5w*_up*MQ..*_ga*ODc4NTgwNDI1LjE3NjA1NjU4ODI.*_ga_21KBGVSV08*czE3NjA1NjU4ODEkbzEkZzAkdDE3NjA1NjU4ODEkajYwJGwwJGgw (last accessed October 15, 2025)

unauthorized third party accessed its network and obtained certain files from its systems from October 21, 2024 to January 13, 2025. ("Data Breach").[3]

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Plaintiff and the proposed Class members, were stolen, including their names, treatment cost information, treatment date information, and health insurance numbers.[4]

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and other individuals' information,

6. Defendant's failure to safeguard Plaintiff's and Class members' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, New Jersey law, and Defendant's implied contract with Plaintiff and Class members to safeguard their Private Information.

7. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

8. Defendant's harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private

[3] The Notice of Data Incident, attached hereto as ***Exhibit A***.
[4] *Id.*

Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

9. Defendant's failure to protect Plaintiff's and Class members' Private Information has harmed and will continue to harm Plaintiff and Class members, causing Plaintiff to seek relief on a Class wide basis.

10. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action against Defendant for negligence, negligence *per se*, breach of fiduciary duty, and breach of implied contract, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

11. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of Louisiana.

12. Defendant Conduent Business Services, LLC, is a New Jersey limited liability company with its headquarters and principal place of business located in Florham Park, New Jersey.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the

Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 putative class members, and at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, namely Plaintiff a citizen of Louisiana. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

14. This Court has personal jurisdiction over Defendant Conduent Business Services, LLC, because its principal place of business is in New Jersey, and it does a significant amount of business in New Jersey.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant Conduent Business Services, LLC has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL BACKGROUND

Defendant Conduent Business Services, LLC's Business

16. Conduent Business Services, LLC provides digital business solutions and services to clients across the commercial, government, and transportation sectors.[5]

[5] https://www.conduent.com/about-conduent/?_gl=1*9qou5w*_up*MQ..*_ga*ODc4NTgwNDI1LjE3NjA1NjU4ODI.*_ga_21KBGVSV08*czE3NjA1NjU4ODEkbzEkZzAkdDE3NjA1NjU4ODEkajYwJGwwJGgw (last accessed October 15, 2025)

17. In connection with the services Defendant provides, Plaintiff and Class members were required to provide sensitive and confidential Private Information, including their names, treatment cost information, treatment date information, and health insurance number, and other sensitive information, that would be held by Conduent in its computer systems.

18. The information held by Conduent at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

19. Upon information and belief, Conduent made promises and representations to Plaintiff and Class members that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Conduent would delete any sensitive information after it was no longer required to maintain it, including through its privacy policies[6].

20. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

[6] *See* Data Privacy at Conduent: "We respect and are committed to safeguarding the confidentiality, data privacy, and security of the information that our customers have entrusted to us, including the confidential information, personally identifiable information, proprietary information, and trade secrets gathered across all of our business operations. Conduent's commitment to data privacy goes beyond the minimum legal and regulatory requirements and strives for best-in-class data protection and privacy management." Available at https://www.conduent.com/privacy-policy/?_gl=1*69126s*_up*MQ..*_ga*ODc4NTgwNDI1LjE3NjA1NjU4ODI.*_ga_21KBGVSV08*czE3NjA1NjU4ODEkbzEkZzEkdDE3NjA1NjU4ODckajU0JGwwJGgw

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

22. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Plaintiff's and Class members' Private Information safe and confidential.

23. Defendant had obligations under the FTC Act, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

24. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Defendant could not provide its services.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable

duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

The Data Breach

26. On or about October 8, 2025, Defendant began notifying Plaintiff and Class members of the Data Breach by sending a Notice of Data Incident ("Notice")[7]:

> **What Happened?** On January 13, 2025, we discovered that we were the victim of a cyber incident that impacted a limited portion of our network. We immediately secured our networks and initiated an investigation with the assistance of third-party forensic experts. Our investigation determined that an unauthorized third party had access to our environment from October 21, 2024, to January 13, 2025, and obtained some files associated with Humana, Inc. Given the nature and complexity of the data involved, Conduent has been working diligently with a dedicated review team, including internal and external experts, to conduct a detailed analysis of the affected files to identify the personal information contained therein.
> We are providing you with this notice upon the recent conclusion of this time-intensive data analysis as your personal information was contained in the affected files.
> **What Information Was Involved.** The affected files contained your name and the following: treatment cost information, treatment date information, and health insurance number. Presently, we have no evidence or indication of actual or attempted misuse of your personal information.

27. To be clear, there are numerous issues with the Conduent Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1) Conduent waited nearly ***nine months*** to notice Plaintiff and Class members of the Data Breach; (2) Conduent's

[7] Exhibit A.

security systems are so insufficient that it does not know the exact date of the Data Breach, and could only provide a time period spanning nearly ***three months***; (3) Conduent fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Conduent continues to maintain is secure; and (4) Conduent fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

28. Furthermore, Defendant's delay in notifying Plaintiff and Class members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in New Jersey. See N.J. Stat. § 56:8-163(a) which requires that the disclosure notification must be "made in the most expedient time possible and without unreasonable delay".[8]

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

[8] While the definition of "reasonable" differs from state to state, it ranges from 30 to 60 days. Defendant failed to meet this requirement by over ***200*** days.

30. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members, including name, treatment cost information, treatment date information, and health insurance number. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

31. Plaintiff further believes her Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

The Defendant Acquires, Collects, and Stores Plaintiff's and Class members' Private Information.

32. In connection with the services that Defendant provides, Plaintiff and Class members were required to give their sensitive and confidential Private Information to Conduent.

33. Conduent retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Conduent would be unable to provide its services.

34. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

35. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

36. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

37. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

38. It is well known that Private Information are invaluable commodities and a frequent target of hackers.

39. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.[9]

[9] ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed December 9, 2024).

40. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

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

42. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

43. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

44. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to hundreds and potentially thousands of individuals' detailed Private Information, and, thus, the

significant number of individuals who would be harmed by the exposure of the unencrypted data.

45. In the Notice, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class members' Private Information. Moreover, once this service expires, Plaintiff and Class members will be forced to pay out of pocket for necessary identity monitoring services.

46. Defendant's offering of credit and identity monitoring establishes that Plaintiff's and Class members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

47. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

48. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

49. As an entity in possession of Plaintiff's and Class members' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply with FTC Guidelines

50. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand

their network's vulnerabilities; and implement policies to correct any security problems.[10]

52. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[11]

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

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

[10] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed October 15, 2025).
[11] *Id.*

these actions further clarify the measures businesses must take to meet their data security obligations.

55. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information.

56. Defendant failed to properly implement basic data security practices.

57. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class members; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with Industry Standards

59. As noted above, experts studying cyber security routinely identify companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

60. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

61. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

62. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including

without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. These foregoing frameworks are existing and applicable industry standards for safeguarding data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Owed Plaintiff and Class members a Duty to Safeguard their Private Information

64. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

65. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private

Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

66. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

67. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

68. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

69. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class members' Risk of Identity Theft

70. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

71. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

72. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

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

74. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

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

76. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their accounts for many years to mitigate the risk of identity theft.

77. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

78. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

79. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

---

[12] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed October 15, 2025).

[13] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed October 15, 2025).

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

Diminution of Value of Private Information

81. Private Information is valuable property.[14] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

82. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change, specifically names.

[14] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed October 15, 2025) ("GAO Report").

83. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[15]

84. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[16]

85. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[17] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[18,19] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[20]

---

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed October 15, 2025).

[16] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[17] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed October 15, 2025).

[18] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed October 15, 2025).

[19] https://datacoup.com/ (last accessed October 15, 2025).

[20] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed October 15, 2025)

86. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

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

88. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

89. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to hundreds and possibly thousands of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

90. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

91. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

93. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

94. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

95. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to provide their Private Information, Plaintiff and other reasonable Class members understood and expected that they were, in part, exchanging their Private Information for Defendant's services, and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

96. Plaintiff is a customer of Conduent. To receive Defendant's services, he was required to provide her Private Information to Conduent.

97. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

98. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

99. Plaintiff learned of the data breach after reviewing the Notice. According to the Notice, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of her name, treatment cost information, treatment date information, and health insurance number.

100. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

101. As a result of the Data Breach, Plaintiff fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that

is contemplated and addressed by law.

102. Additionally, Plaintiff has suffered actual injury in the form of an increase in spam calls following the Breach. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud

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

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

105. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

106. Plaintiff brings this suit on behalf of herself and a Class of similarly situated individuals pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3), on behalf of the following class:

> All individuals whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

107. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

108. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

109. **Numerosity.** The Class members are so numerous that joinder of all members is impracticable. While the exact number is unknown to Plaintiff, it is believed to be in the hundreds, and possibly even thousands. The identities of Class members are ascertainable through Defendant's records, Class members' records, publication notice, self-identification, and other means.

110. **Commonality.** Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendant has a duty to protect the Private Information of Plaintiff and Class members;

b. Whether Defendant has respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant has respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

111. **Typicality.** Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

112. **Policies Generally Applicable to the Class.** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

113. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the Class members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to the Class members and the infringement of the rights and the damages she has suffered is typical of other Class members. Plaintiff

has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

114. **Superiority and Manageability**. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

115. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be

recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

116. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

117. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

118. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

119. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

120. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard Plaintiff's and Class members' Private Information; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach

121. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION
COUNT I
Negligence
(On behalf of Plaintiff and the Class)

122. Plaintiff hereby repeats and realleges paragraphs 1 through 121 of this Complaint and incorporates them by reference herein.

123. Defendant requires Plaintiff and Class members, to submit non-public Private Information in connection with the services Defendant provides.

124. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business practices.

125. Plaintiff and Class members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

126. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

127. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

128. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

129. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential Private Information, a necessary part of employment with Defendant.

130. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also

because Defendant is bound by industry standards to protect confidential Private Information.

131. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

132. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

133. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

134. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

135. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

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

137. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

138. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

139. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

140. Defendant's duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or

where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

141. Defendant has admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

142. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

143. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

144. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

145. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

146. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Class)

148. Plaintiff hereby repeats and realleges paragraphs 1 through 121 of this Complaint and incorporates them by reference herein.

149. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

150. Defendant breached its duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

151. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

152. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

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

154. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

155. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class)

156. Plaintiff hereby repeats and realleges paragraphs 1 through 121 of this Complaint and incorporates them by reference herein.

157. Plaintiff and the other Class members gave Defendant their Private Information believing that Defendant would protect that information. Plaintiff and the other Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and the other Class members' Private Information created a fiduciary relationship between Defendant on the one hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of Plaintiff and Class members, which includes

safeguarding and protecting Plaintiff's and the other Class members' Private Information.

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

159. Defendant has a fiduciary duty to act for the benefit of Plaintiff and the other Class members upon matters within the scope of their relationship. It breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class members' Private Information and otherwise failing to safeguard Plaintiff's and the other Class members' Private Information that they collected.

160. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and the other 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, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from

unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data breach; (vii) loss of potential value of their Private Information; (viii) overpayment for the services that were received without adequate data security.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

161. Plaintiff hereby repeats and realleges paragraphs 1 through 121 of this Complaint and incorporates them by reference herein.

162. Plaintiff and Class members were required to provide their Private Information to Defendant in connection with the services Defendant provides.

163. In turn, Defendant impliedly promised and represented to protect Plaintiff's and Class members' Private Information through adequate data security measures, including through its privacy policies.

164. Plaintiff and the Class members accepted Defendant's offer by providing Private Information to Defendant in exchange for services and data security assurances.

165. Plaintiff and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

166. Defendant materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

167. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

168. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

169. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

170. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith

and fair dealing.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance

with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and security checks;

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

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their

confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

D. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: October 28, 2025.

Respectfully submitted,

By: */s/Leanna Loginov*

Leanna A. Loginov, Esq. (NJ Bar 389742022)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Telephone: 305-479-2299
lloginov@shamisgentile.com

Attorney for Plaintiff and the Putative Class