UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

REAGAN SMITH, on behalf of himself and all others similarly situated, Plaintiff, v. CONDUENT INCORPORATED, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Reagan Smith ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, Conduent Incorporated, ("Conduent" or "Defendant"):

INTRODUCTION

1. On January 13, 2025, Conduent, an American business services provider headquartered in New Jersey that provides digital platforms for both private businesses and the government, discovered that it lost control over its computer network and the highly sensitive personal information stored on its computer network in a data breach perpetrated by cybercriminals ("Data Breach"). Upon information and belief, the Data Breach has impacted at least 462,000 current and former customers.[1]

2. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to customers' personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") between October 21, 2024, until January

[1] DataBreaches.Net, *Protected health information of 462,000 members of Blue Cross Blue Shield of Montana involved in Conduent data breach*, https://databreaches.net/2025/10/22/protected-health-information-of-462000-members-of-blue-cross-blue-shield-of-montana-involved-in-conduent-data-breach/ (last visited October 24, 2025).

13, 2025, and "obtained files."[2]

3. On or about April 9, 2025, three months after discovering the breach, Conduent finally reported the incident in a Form 8-K filing with the United States Securities and Exchange Commission ("Form 8-K Notice").

4. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the Private Information of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information—rendering it an easy target for cybercriminals.

5. Defendant's Form 8-K Notice and Data Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its customers how many people were impacted and how the breach happened.

6. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Private Information misuse.

8. In failing to adequately protect its customers' information and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former customers.

9. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber

[2] Sample Breach Notice, Attorney general of New Hampshire, conduent-business-services-20251008.pdf (last visited October 24, 2025).

security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Private Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff is a customer of Defendant's and a Data Breach victim.

11. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

12. Plaintiff, Reagan Smith is a natural person and citizen of Wisconsin, residing in Milwaukee, Wisconsin, where she intends to remain.

13. Defendant, Conduent Incorporated, is a company incorporated in Delaware, with its principal place of business located at 100 Campus Drive, Suite 200 Florham Park, New Jersey 07932.

JURISDICTION & VENUE

14. 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. Plaintiff and Defendant are of different states. And there are over 100 putative Class members.

15. This Court has personal jurisdiction over Defendant because it is headquartered in New Jersey, regularly conducts business in New Jersey, and has sufficient minimum contacts in New Jersey.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Conduent

17. Conduent touts that it "delivers digital business solutions and services spanning the commercial, government and transportation spectrum – creating valuable outcomes for its clients and the millions of people who count on them."[3] It boasts a staggering annual revenue of $3.4 billion.[4]

18. On information and belief, Conduent accumulates highly sensitive Private Information of its current and former customers.

19. In collecting and maintaining its customers' Private Information, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Private Information.

20. Conduent understood the need to protect its current and former customers' Private Information and prioritize its data security.

21. Indeed, Conduent promises in its privacy policy that **"**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."[5]

22. Conduent further boasts that:

[3] Conduent, https://www.linkedin.com/company/conduent/ (last visited October 27, 2025).
[4]Zoominfo, Conduent, https://www.zoominfo.com/c/conduent-inc/399034598 (last visited October 27, 2025).
[5] Conduent, Privacy policy, https://www.conduent.com/privacy-policy/#adchoices (October 27, 2025)

> 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. This commitment is overseen at the executive level by the Chief Privacy Officer who reports to the General Counsel and the Chief Information Security Officer who reports to the Chief Information Officer (with the General Counsel and Chief Information Officer both reporting directly to the Chief Executive Officer of the company.) The Board receives reports from both the Chief Privacy Officer and Chief Security Officer. The Risk Oversight Committee agenda includes coverage of data privacy at every meeting.

23. Despite recognizing its duty to do so, on information and belief, Conduent has not implemented reasonably cybersecurity safeguards or policies to protect customers' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to customers' Private Information.

Conduent Failed to Safeguard Customers' Private Information

24. Plaintiff is a customer of Conduent. As a condition of receiving Conduent's services, Plaintiff provided Defendant with her Private Information. Defendant used that Private Information to facilitate its services to Plaintiff and required Plaintiff to provide that Private Information to obtain its services.

25. On information and belief, Conduent collects and maintains customers' unencrypted Private Information in its computer systems.

26. In collecting and maintaining Private Information, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

27. According to its Form 8-K notice, on January 13, 2025, Defendant "experienced an operational disruption and learned that a threat actor [had] gained unauthorized access [to a] portion of [Conduent's] environment." Following an internal investigation, Defendant discovered that "the threat actor exfiltrated a set of files" and admitted that "the data sets contained a significant number of individuals' personal information associated with our clients' end-users."

28. According to Defendant's Breach Notice, it's investigation into the incident revealed that "an unauthorized third party had access to our environment from October 21, 2024, to January 13, 2025, and obtained some files." Thus, cybercriminals had access to individuals' Private Information for almost *three months*, during which time they were able to steal Private Information from Defendant's systems.

29. In other words, Defendant's cyber and data security systems were completely inadequate in that it allowed cybercriminals to obtain files containing a treasure trove of hundreds of thousands of its customers' highly sensitive Private Information, including names, birth dates, Social Security numbers, treatment and diagnosis codes, provider names, and claims amounts.[6]

30. Despite this, Defendant waited until October 2025—an entire year after the Data Breach began—to begin notifying victims that their Private Information had been compromised and stolen during the Data Breach. *See* Exhibit A.

31. Defendant's Breach Noticed acknowledged the increased risk faced by victims of the Data Breach when it urged those affected to "remain vigilant against the potential for identity theft and fraud and to monitor your credit reports for any suspicious activity." Ex. A.

32. Because of Defendant's Data Breach, the sensitive Private Information of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

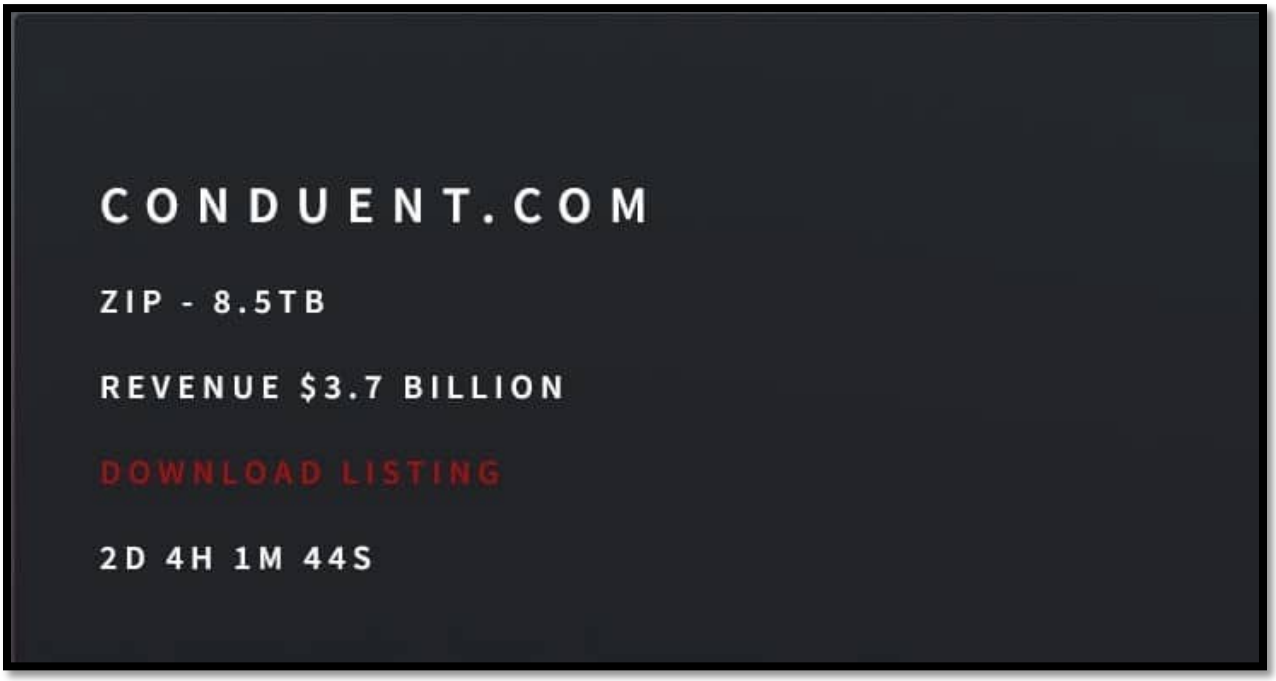
33. The notorious SafePay ransomware gang claimed responsibility for the cyberattack. SafePay is one of the most active ransomware actors that first surfaced in October 2024 and has since become infamous for targeting multiple business sectors around the world.[7] Defendant, self-

[6] HIPAA Journal, https://www.hipaajournal.com/blue-cross-blue-shield-montana-data-breach/ (last visited October 24, 2025).
[7] Red Piranha, https://redpiranha.net/news/what-is-safepay-ransomware-everything-you-need-know (October 27, 2025).

proclaimed global leader knew or should have known of the tactics that groups like SafePay employ.

34. With the Sensitive Information secured and stolen by SafePay, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant has provided no public information on the ransom demand or payment.

35. On the presumed deadline of SafePay's ransom demand, SafePay released information obtained from the Breach, up to 8.5 Terabyte worth of information, on a data leak page.[8]



36. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Private Information for theft and sale on the dark web.

37. Despite its duties to safeguard Private Information, Defendant did not in fact follow industry standard practices in securing customers' Private Information, as evidenced by the Data

[8] Comparitech, https://www.comparitech.com/news/another-ransomware-gang-says-it-breached-it-giant-conduent/ (October 27, 2025).

Breach.

38. Typically, in response to a Data Breach, Defendant will make promises of additionally implemented cybersecurity practices to prevent any future data breaches from occurring. However, Defendant's Breach Notice failed to mention any improved cybersecurity practices. Regardless, even if Defendant were to take additional cybersecurity measure, these measures should have been in place before the Data Breach.

39. On information and belief, Conduent plans to offer several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach likely involves Private Information that cannot be changed, such as Social Security numbers.

40. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Private Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' Private Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

43. It is well known that Private Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[9]

45. In light of recent high profile data breaches, including, 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 its electronic records would be targeted by cybercriminals.

46. 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.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

48. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

[9] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 4, 2023).

49. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[10]

50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[11]

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[12]

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

---

[10] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed October 27, 2025).

[11] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed October 27, 2025).

[12] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed October 27, 2025).

53. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands of its current and former employes in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

54. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

55. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its customers' Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

Consumers Prioritize Data Security

56. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[13] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[14]

[13] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited October 27, 2025).
[14] *Id*. at 3.

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[15]

c. 89% of consumers stated that "I care about data privacy."[16]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[17]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[18]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[19]

57. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Private Information, including Plaintiff and the Class's Private Information was important to its patients.

Plaintiff's Experience and Injuries

58. Plaintiff is a customer of Conduent. As a condition of receiving Conduent's services, Plaintiff provided Defendant with her Private Information. Defendant used that Private Information to facilitate its services to Plaintiff and required Plaintiff to provide that Private Information to obtain its services.

59. Plaintiff provided her Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

---

[15] *Id*.
[16] *Id*. at 9.
[17] *Id*.
[18] *Id*.
[19] *Id*. at 11.

60. On information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

61. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about the Breach.

62. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and sale on the dark web.

63. Plaintiff suffered actual injury from the exposure of her Private Information — which violates her rights to privacy.

64. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

65. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit information.

66. Plaintiff has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration 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 the law contemplates and addresses.

67. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third

parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

68. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[20] On information and belief, the fraudulent credit inquiries Plaintiff experienced were a result of the Data Breach.

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

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

70. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

71. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort

[20] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited October 27, 2025).

expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

72. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

73. The value of Plaintiff's and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

74. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

75. It can take victims years to spot identity or Private Information theft, giving criminals plenty of time to use that information for cash.

76. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

77. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

78. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

79. Defendant disclosed the Private Information of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

80. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach

exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

81. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

82. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

83. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

84. The FTC recommends that companies not maintain 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.

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

86. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

87. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep individuals' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [21]

88. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[22]

89. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

[21] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[22] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

90. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Failed to Follow Industry Standards

91. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: 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.

92. Other industry standard best practices 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; and training staff regarding critical points.

93. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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).

94. These frameworks are applicable and accepted industry standards. And by failing

to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

95. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> **All individuals residing in the United States whose Private Information was compromised in Defendant's Data Breach, including all those who received notice of the breach.**

96. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

97. Plaintiff reserves the right to amend the class definition.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of approximately 462,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. 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;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

98. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

99. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

100. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

101. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

102. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

103. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' Private Information.

104. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect

the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

105. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

106. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

107. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

108. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

109. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

110. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

111. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

112. Defendant breached these duties as evidenced by the Data Breach.

113. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

114. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

115. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

116. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

117. As a direct and traceable result of Defendant's negligence and/or negligent

supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

118. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence *per se*
(On Behalf of Plaintiff and the Class)

119. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

120. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

121. Section 5 of the FTC Act 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 the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive Private Information.

122. Defendant breached its respective 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 Private Information.

123. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

124. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

125. Similarly, Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients and their employees, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

126. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

127. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and

Class Members would not have been injured.

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

129. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

130. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

131. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

132. Defendant offered services to Plaintiff and members of the Class if, as a condition of providing these services, Plaintiff and members of the Class provided Defendant with their Private Information.

133. In turn, Defendant agreed it would not disclose the Private Information it collects to unauthorized persons. Defendant also promised to safeguard customers' Private Information.

134. Plaintiff and the members of the Class accepted Defendant's offer by providing Private Information to Defendant in exchange for financial services with Defendant.

135. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

136. Plaintiff and the members of the Class would not have entrusted their Private

Information to Defendant in the absence of such an agreement with Defendant.

137. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Private Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

138. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

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

140. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon 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 in addition to its form.

141. Subterfuge and evasion violate the obligation of good faith in performance even

when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

142. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

143. In these and other ways, Defendant violated its duty of good faith and fair dealing.

144. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

145. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

146. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

147. This claim is plead in the alternative to the breach of implied contractual duty claim.

148. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of monetary payment. Defendant also benefited from the receipt of Plaintiff's and the Class's Private Information, as this was used to facilitate financial services.

149. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

150. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information or worked for Defendant at the

payrates they did had they known Defendant would not adequately protect their Private Information.

151. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

152. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

153. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

154. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep this information confidential.

155. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

156. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

157. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

158. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

159. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

160. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

161. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

162. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their Private Information are still maintained by Defendant with its inadequate cybersecurity system and policies.

163. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

164. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SIXTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of the Plaintiff and the Class)

165. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

166. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff's and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

167. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

168. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

169. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

170. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

171. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: October 27, 2025,

Respectfully Submitted,

/s/ *Mark K. Svensson*
Mark K. Svensson (NJ Bar No.: 380202021)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
405 East 50th Street, Suite 408
New York, NY 10022
Tel: (866) 252-0878
msvensson@milberg.com

Samuel J. Strauss*
Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class