CAUSE NO.

CLIFTON TYLER ALLEN, STEVEN GETMAN, and ROBIN RAYCHELLE PETTY, *individually and on behalf of all others similarly situated*, Plaintiffs, v. AIS INFOSOURCE, L.P., Defendant.	IN THE DISTRICT COURT HARRIS COUNTY, TEXAS _____ JUDICIAL DISTRICT

PLAINTIFFS CLASS ACTION PETITION

Plaintiffs Clifton Tyler Allen, Steven Getman, and Robin Raychelle Petty ("Plaintiffs") bring this Class Action Complaint ("Complaint") against AIS InfoSource, L.P. ("AIS" or "Defendant"), for its failure to properly secure and safeguard Plaintiffs and Class Members' personally identifiable information stored within Defendant's information network, including without limitation, names, addresses, and Social Security numbers ("Private Information" or "PII").

Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and facts that are a matter of public record.

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant, AIS.

2. Plaintiffs further seek to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry standards.

3. On information and belief, on or around February 17, 2025, AIS became aware of a data security incident, which resulted in unauthorized access to certain personal and/or protected information maintained by AIS, resulting in the unauthorized disclosure of the Private Information of Plaintiffs and the Class Members, including names, Social Security numbers, and financial account information (the "Data Breach").

4. As explained below, Plaintiffs and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by AIS, including monetary damages, out-of-pocket expenses, and damages associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiffs and the Class also now forever face an amplified risk of misuse, fraud, and identity theft due to their sensitive Private Information falling into the hands of cybercriminals because of the tortious conduct of Defendant.

5. On information and belief, Plaintiffs' Private Information is available on the Dark Web as a result of the Data Breach.

6. On behalf of themselves and the Class preliminarily defined below, Plaintiffs bring causes of action for: (i) Negligence and Negligence *Per Se*; (ii) Intrusion Upon Seclusion/Invasion of Privacy; (iii) Unjust Enrichment and (iv) Declaratory Judgment and Injunctive Relief. Plaintiffs seek damages and injunctive and declaratory relief arising from AIS's failure to adequately protect their highly sensitive Private Information.

NATURE OF THE ACTION

7. Plaintiffs bring this class action lawsuit against Defendant, AIS, for its failure to properly secure and safeguard the PII of Plaintiffs and other similarly situated current and former customers of companies that use AIS's services (collectively defined herein as the "Class" or

"Class Members"). That PII includes names, Social Security numbers, and financial account information from cybercriminals.

8. According to its website, AIS helps reduce costs, improve compliance, and mitigate risk by automating processes and providing data management services to financial institutions.[1]

9. As part of its business, Defendant receives and maintains the Private Information of thousands of its current and former customers (and/or the current and former customers of Defendant's institutional clients).

10. Plaintiffs and Class Members' sensitive personal information—which they entrusted to Defendant through Defendant's institutional clients on the mutual understanding that Defendant would protect against disclosure— was targeted, compromised, and unlawfully accessed due to the Data Breach.

11. Under state and federal law, businesses like Defendant have duties to protect the PII of Defendant's current and former customers (and/or the current and former customers of Defendant's institutional clients)—and to notify them about data breaches.

12. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, financial identity theft, invasion of their private health matters and other long-term issues.

13. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly

[1] https://aisinfo.com/about-us

impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

14. Mitigating that risk requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

15. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

16. According to AIS's website, "[t]he safety of our clients' data is our top priority. That's why we believe that no other company in this industry has invested in data security like AIS. Much like our clients, data security is a key element to our own business."[2]

17. The breach involved the divulgence of Private Information of Defendant's clients including, but not limited to, their: names, Social Security Numbers, and financial information.

18. According to the Breach Notification Letter ("Notice Letter") distributed by AIS:

> On February 17, 2025, AIS identified suspicious activity in our network and promptly took measures to mitigate the risk of further activity. AIS quickly initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation revealed that the earliest known unauthorized activity in our systems occurred between February 16, 2025, and February 21, 2025. Through the investigation, we determined that an unauthorized actor gained access to our environment and took a limited subset of data. Therefore, AIS retained a third-party to complete a comprehensive review of the data involved to determine what information was at issue and to whom it belonged. On May 15, 2025, AIS determined that information related to you was included in the data and worked to gather contact information so that direct notice could be provided. On June 13, 2025, AIS received sufficient information to provide direct notice to you.[3]

[2]https://aisinfo.com/about-us/security-standards
[3]The Breach Notification Letter can be found here:
https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8319b85b-9339-46a0-a681-6e282414d676.html

19. The data could be used for malicious purposes in the wrong hands, such as phishing and social engineering.

20. A data breach is a type of cybersecurity intrusion whereby the cybercriminal deploys "ransomware" on a given entity's computer system and data storage network. Ransomware that works to "lock" access to a given computer system or data storage network until the entity pays a ransom, usually in untraceable cryptocurrency, in order to regain access.

21. As a direct and proximate result of Defendant's failure to implement and to follow basic security procedures, Plaintiffs and Class Members' Private Information now appears to be in the hands of cybercriminals.

22. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their privacy, Private Information being disseminated on the dark web, and similar forms of criminal mischief - risks which may last for the rest of their lives.

23. Plaintiffs and Class Members have also suffered concrete injuries in fact including, but not limited to, lost or diminished value of Private Information, lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, and actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails.

24. Consequently, Plaintiffs and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal

consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

25. Plaintiffs, on behalf of themselves and all others similarly situated, therefore bring claims for (i) Negligence and Negligence *Per Se*; (ii) Implied Breach of Contract; (iii) Breach of Fiduciary Duty; (iv) Intrusion Upon Seclusion/Invasion of Privacy; (v) Unjust Enrichment and (vi) Declaratory Judgment and Injunctive Relief. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendant's custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Plaintiffs

22. Plaintiff Clifton Tyler Allen is, and at all times mentioned herein, an individual citizen residing in Cookeville, Tennessee.

23. Plaintiff Steven Getman is, and at all times mentioned herein, an individual citizen residing in Atlanta, Georgia.

24. Plaintiff Robin Raychelle Petty is, and at all times mentioned herein, an individual citizen residing in Plainfield, Indiana.

Defendant AIS InfoSource, L.P.

25. Defendant, AIS InfoSource, L.P., is a Texas corporation with its corporate headquarters in Texas. Its principal place of business is located at: 5847 San Felipe Street, Houston, Texas, 77057.

JURISDICTION & VENUE

26. This Court has subject matter jurisdiction over this action because Defendant's negligent conduct occurred in Jefferson County, Texas. Plaintiffs have been damaged in a sum within the jurisdictional limits of this Court. Pursuant to Texas Rule of Civil Procedure 47, Plaintiffs seek monetary relief over $1,000,000.00. Plaintiffs reserve the right to amend their petition during and/or after the discovery process. Due to the complexity of the case, discovery should be conducted pursuant to a discovery control plan under Level 3. *See* Texas Rule of Civil Procedure 190.4.

27. This Court has personal jurisdiction over Defendant because it is a resident of the State of Texas.

28. Venue is proper in this County under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in Jefferson County, Texas, and because Defendant maintains its principal place of business in Jefferson County.

29. Upon information and belief, each of Plaintiffs' individual damages are less than $75,000.

30. Upon information and belief, at least two-thirds of the Class (defined infra) are residents of Texas.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collects a Significant Amount of Private Information.

29. Plaintiffs and Class Members are current and former customers of Defendant's financial institution clients.

30. As part of its business, Defendant receives and maintains the Private Information of its current and former customers (and/or the current and former customers of Defendant's institutional clients).

31. Upon information and belief, in the course of collecting Private Information from clients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security from the data it collected from clients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

32. Defendant states on its website that: "The safety of our clients' data is our top priority. That's why we believe that no other company in this industry has invested in data security like AIS. Much like our clients, data security is a key element to our own business. We are audited on a monthly basis by major financial institutions and continue to surpass the security expectations for our clients."

33. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its clients, Defendant is required to keep clients' Private Information private; comply with industry standards related to data security and the maintenance of their clients' Private Information; inform their clients of its legal duties relating to data security; comply with all federal and state laws protecting clients' Private Information; only use and release clients' Private Information for reasons that relate to the services they provide; and provide adequate notice to clients if their Private Information is disclosed without authorization.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs and Class Members' Private Information from unauthorized disclosure and exfiltration.

35. Without the required submission of Private Information from Plaintiffs and Class Members, Defendant could not perform the services it provides.

36. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

37. Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs and Class Members' Private Information.

B. The Data Breach

39. On or about June 30, 2025, the Defendant issued the following statement in the Notice Letter:

> On February 17, 2025, AIS identified suspicious activity in our network and promptly took measures to mitigate the risk of further activity. AIS quickly initiated an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation revealed that the earliest known unauthorized activity in our systems occurred between February 16, 2025, and February 21, 2025. Through the investigation, we determined that an unauthorized actor gained access to our environment and took a limited subset of data. Therefore, AIS retained a third-party to complete a comprehensive review of the data involved to determine what information was at issue and to whom it belonged. On May 15, 2025, AIS determined that information related to you was included in the data and worked to gather contact information so that direct notice could be provided. On June 13, 2025, AIS received sufficient information to provide direct notice to you.[4]

40. Omitted from news sources is who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been

[4] The Notice Letter is available here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8319b85b-9339-46a0-a681-6e282414d676.html

explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

41. 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 Texas. See Tex. Bus. & Com. Code § 521.035(c), which requires that the disclosure be "immediately after discovering the breach..."

42. Defendant's 133-day delay in providing its Notice Letter to Plaintiff and Class Members after discovering the Data Breach is in violation of Tex. Bus. & Com. Code § 521.035(c).

43. Defendant has obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiffs and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

44. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its clients' PII.

C. Defendant Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

44. Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

45. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial) against the individuals whose Private Information was compromised.

46. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, and Anthem, as well as countless others in the industry.

47. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5]

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

49. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[6]

50. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

51. Recently, in 2024, 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[8] In 2024, the financial services industry that Defendant operates in was the most targeted industry for data compromises among all sectors measured.[9]

52. Indeed, cybercriminals seek out PII at a greater rate than other sources of personal

[5] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Feb. 9, 2026).
[6] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://go.flashpointintel.com/docs/2021-Year-End-Report-data-breach-quickview (last visited Feb. 9, 2026).
[7] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 9, 2026).
[8] *2024 Data Breach Report*, ITRC (Identity Theft Resource Center) (January 2025), *available at* https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last accessed Feb. 9, 2026).
[9] *Id.*

information.[13]

53. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's clients especially vulnerable to identity theft, tax fraud, financial fraud, credit and bank fraud and more.

54. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: personal "records are a gold mine for criminals—they can access a client's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PII records can go from $20 say up to—we've even seen $60 or $70."[10]

55. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $100.[11] According to Experian:

> Having your records stolen in a data breach can be a prescription for financial disaster. If scam artists break into networks and grab your PII information, they can impersonate you to get other financial services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC.

[10] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Poniman Study Shows*, IDX (May 14, 2015), https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[11] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PWC.COM (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Victims of data breaches may also find themselves threatened with being charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[12]

56. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

57. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

58. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

[12] Brian O'Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one.

59. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[13] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

60. Identity thieves can also use stolen personal information such as Social Security numbers and PII for a variety of crimes, including identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

61. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud: A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, and it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

[13] *See* https://www.identitytheft.gov/Steps

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

62. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

63. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

64. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is misused.

65. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[16]

---

[14] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 9, 2026).

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-hasmillionsworrying-about-identity-theft.

[16] *Report to Congressional Requesters, 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 visited Feb. 9, 2026).

66. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

67. Based on the value of its clients' PII to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

D. The Data Breach was Preventable.

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

69. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

70. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented numerous measures as recommended by the United States Government, including but not limited to:

- Implementing an awareness and training program.
- Enabling strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain

Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scanning all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configuring firewalls to block access to known malicious IP addresses.
- Setting anti-virus and anti-malware programs to conduct regular scans automatically.
- Managing the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.[17]

71. Given that Defendant was storing the Private Information of its current and former clients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

72. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of likely thousands of individuals, including that of Plaintiffs and Class Members.

E. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices.

73. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain

[17] How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Feb. 9, 2026).

reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

74. 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.[18]

75. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[19]

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.

77. 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[18] U.S. Fed. Trade Comm'n, *Start with Security – A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[19] U.S. Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

78. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to client's PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

79. Defendant was at all times fully aware of its obligations to protect the PII of clients because of its position as a data service provider, which gave it direct access to reams of client PII.

80. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Violated Industry Standards.

81. Several best practices have been identified that, at a minimum, should be implemented by data service provider entities 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. AIS failed to follow these industry best practices, including a failure to implement multi-factor authentication.

82. Other best cybersecurity practices that are standard for data service providers 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.

83. 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.

84. These foregoing frameworks are existing and applicable industry standards for data service provider entities, 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.

G. The Monetary Value of Plaintiffs & Class Members' Private Information.

85. As a result of Defendant's failures, Plaintiffs and Class Members are at substantially increased risk of suffering identity theft and fraud or misuse of their Private Information.

86. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identifying fraud is only about 3%.[20]

87. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

88. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal

[20] Stu Showerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWB4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Feb. 9, 2026).

Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

89. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[22]

90. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbor, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[23]

91. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

---

[21] U.S. Fed. Trade Comm'n, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Feb. 7, 2001), https://www.ftc.gov/legal-library/browse/federal-register-notices/public-workshop-information-marketplace-merging-exchanging-consumer-data.

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[23] *Statement of FTC Commissioner Pamela Jones Harbor—Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploringprivacy-roundtable/091207privacyroundtable.pdf.

[24] Angwin & Steel, *supra* note 30.

92. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

93. The value of Plaintiffs' and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[26]

94. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's conditions or victim settlements.

95. Identity theft can result in inaccuracies in clients' records and costly false claims. It can also have life-threatening consequences. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal files due to the thief's activities."[27]

96. The ramifications of Defendant's failure to keep its clients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

97. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[28]

---

[25] *See* U.S. Depot of Justice, *Victims of Identity Theft* (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[26] *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector.
[27] Michael Olive, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft.
[28] *See Medical ID Theft Checklist*, https://www.identityforce.com/blog/medical-id-theftchecklist-2.

98. Indeed, when compromised, Social Security numbers and financial information is among the most private and personally consequential.

99. A report focusing on data breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs. [29]

100. Almost 50% of the surveyed victims lost their insurance coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including identity theft, have a crippling effect on individuals and detrimentally impact the economy as a whole.[30]

101. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including identity theft) and fraud.

102. Upon information and good faith belief, if Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of clients within their systems.

103. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great

[29] Elinor Mills, *Study: Medical identity theft is costly for victims* (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims.
[30] *Id.*

value to hackers and thieves.

104. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[31] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[32]

105. Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that can be misused.

106. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

107. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

108. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

[31] U.S. Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38 (Dec. 2010), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[32] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

109. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

110. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

H. Plaintiffs & Class Members Have Suffered Compensable Damages.

111. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways.

112. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

113. In order to mitigate against the risks of identity theft and fraud, Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

114. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

115. Further, the value of Plaintiffs and Class Members' PII has been diminished by its exposure in the Data Breach.

116. Plaintiffs and Class Members now face a greater risk of identity theft, including financial identity theft.

117. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its clients' PII.

118. Plaintiffs and Class Members have suffered emotional distress because of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

119. Plaintiffs and Class Members also did not receive the full benefit of their bargain when paying for services. Instead, they received services of a diminished value to those described in their agreements with Defendant. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

120. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over

its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

121. Finally, in addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFFS EXPERIENCE

Plaintiff Clifton Tyler Allen's Experience

122. Plaintiff Clifton Tyler Allen is a customer of one of Defendant's financial institution clients.

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

124. Plaintiff Allen provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

125. Plaintiff Allen reasonably understood that in exchange for providing Defendant his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

126. Plaintiff Allen received the Notice, by U.S. mail, directly from Defendant, dated July 21, 2025. According to the Notice, Plaintiff Allen's Private Information was improperly accessed and obtained by unauthorized third parties, including name, Social Security number, and financial account information.

127. As a result of the Data Breach, Plaintiff Allen made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity.

128. Plaintiff Allen has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff 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.

129. Subsequent to the Data Breach, Plaintiff Allen has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) financial fraud; (v)lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

130. The Data Breach has caused Plaintiff Allen to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

131. Moreover, Plaintiff Allen suffered actual injury in the form of experiencing an increase in spam calls, which, upon information and belief, was caused by the Data Breach. This misuse of his 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, 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.

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

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

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

Plaintiff Steven Getman's Experience

135. Plaintiff Steven Getman is a customer of one of Defendant's financial institution clients.

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

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

138. Plaintiff Getman provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

139. Plaintiff Getman reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

140. Plaintiff Getman received the Notice, by U.S. mail, directly from Defendant, dated July 21, 2025. According to the Notice, Plaintiff Getman's Private Information was improperly accessed and obtained by unauthorized third parties, including name, Social Security number, and financial account information.

141. As a result of the Data Breach, Plaintiff Getman made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity. Plaintiff Getman has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff Getman 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.

142. Subsequent to the Data Breach, Plaintiff Getman has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) financial fraud; (v)lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third

parties to access and abuse; and (b) remains backed up 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.

143. The Data Breach has caused Plaintiff Getman to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

144. Moreover, Plaintiff Getman suffered actual injury in the form of experiencing an increase in spam calls, which, upon information and belief, was caused by the Data Breach. This misuse of his 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, 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.

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

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

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

Plaintiff Robin Raychelle Petty's Experience

148. Plaintiff Robin Raychelle Petty is a customer of one of Defendant's financial institution clients.

149. As a condition of obtaining services from Defendant's financial institution client, she was required to provide her Private Information to Defendant.

150. Upon information and good faith belief, Defendant maintained Plaintiff Petty's Private Information in its systems at the time of the Data Breach.

151. Plaintiff Petty received a notice letter from Defendant dated July 21, 2025 informing her that her name, Social Security Number, and financial information was impacted in the Data Breach.

152. Plaintiff Petty is very careful about sharing her sensitive Private Information. Plaintiff Petty stores any documents containing Plaintiff Petty's Private Information in a safe and secure location. Plaintiff Petty has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Petty would not have entrusted Plaintiff Petty's Private Information to Defendant had she known of Defendant's lax data security policies.

153. As a result of the Data Breach, Plaintiff Petty made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Petty 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.

154. Plaintiff Petty estimates she has spent between twelve and fifteen hours on the Data Breach. She has spent time going to her bank, researching the Data Breach, as well as looking into the credit monitoring options offered by Defendant.

155. Plaintiff Petty suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (I) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

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

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

158. Plaintiff Petty 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.

CLASS ALLEGATIONS

159. Plaintiffs bring this action individually and on behalf of all other persons similarly situated.

160. Specifically, Plaintiffs propose the following class definitions, subject to amendment as appropriate:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised in the Data Breach with AIS Services, Inc. which took place on or around February 16, 2025 (the "Nationwide Class").

161. Excluded from the Classes are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, all judges assigned to hear any aspect of this litigation, their immediate family members, and those individuals who make a timely and effective election to be excluded from this matter using the correct protocol for opting out.

162. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

163. **Numerosity:** Plaintiffs are informed and believe there are likely hundreds if not thousands of individuals of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

164. **Commonality:** This action involved questions of law and fact common to the Class that predominate over any questions affecting solely individual members of the Class. Such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach.

b. Whether Defendant had a duty to protect the PII of Plaintiffs and Class Members.

c. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties.

d. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members for non-business purposes.

e. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members.

f. Whether and when Defendant actually learned of the Data Breach.

g. Whether Defendant was negligent in collecting and storing Plaintiffs and Class Members' PII, and breached its duties thereby.

h. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised.

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised.

j. 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.

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur.

l. Whether Defendant was negligent and that negligence resulted in the Data Breach.

m. Whether Defendant entered into an implied contract with Plaintiffs and Class Members.

n. Whether Defendant breached that contract by failing to adequately safeguard Plaintiffs and Class Members' PII.

o. Whether Defendant was unjustly enriched.

p. Whether Plaintiffs and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

q. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

165. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all clients, or family members or caregivers of clients, of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

166. **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 Plaintiffs' challenges of these policies hinge on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

167. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

168. **Superiority and Manageability:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

169. 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.

170. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs 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 Plaintiffs are 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.

171. 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.

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

173. 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.

174. 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.

175. Likewise, particular issues 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 Plaintiffs and the class of the Data Breach.

b. Whether Defendant owed a legal duty to Plaintiffs 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 client Private Information; and whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

176. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the

Class. If Defendant breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

177. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class.

178. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

CAUSES OF ACTION

FIRST COUNT -NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and all Class Members)

179. Plaintiffs repeat and re-allege each and every factual allegation contained in the previous paragraphs 1 through 178.

180. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiffs and Class Members' PII on its computer systems and networks.

181. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession.

b. to protect Plaintiffs and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices.

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

182. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

183. Defendant knew or should have known of the risks inherent in collecting and storing PII , the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

184. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiffs and Class Members' PII.

185. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiffs and Class Members had entrusted to it.

186. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII.

187. Because Defendant knew that a breach of its systems could damage hundreds of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained thereon.

188. Plaintiffs and Class Members' willingness to entrust Defendant with its PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

189. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs and Class Members' PII and promptly notify them

about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiffs and/or the remaining Class Members.

190. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII.

b. by failing to timely and accurately disclose that Plaintiffs and Class Members' PII had been improperly acquired or accessed.

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII.

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiffs and Class Members' PII, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PII longer than absolutely necessary.

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class Members' PII.

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Plaintiffs and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

191. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

192. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

193. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs and Class Members' PII and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and Class Members. Plaintiffs and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

194. Defendants' wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

195. The damages Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

196. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) 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 PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

197. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

198. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to (I) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the

compromise, publication and/or theft of their PII , (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII , (v) lost opportunity costs associated with effort expended and the loss of productivity 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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

199. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs 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 noneconomic losses.

200. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, 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 PII in its continued possession.

SECOND COUNT - INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On Behalf of Plaintiffs and All Class Members)

201. Plaintiffs repeat and re-allege each and every factual allegation contained in the previous paragraphs 1 through 178.

202. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.
>
> Restatement (Second) of Torts§ 652B (1977).

203. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII that Defendant mishandled.

204. Defendants' conduct as alleged above intruded upon Plaintiffs and Class Members' seclusion under common law.

205. By intentionally failing to keep Plaintiffs and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class Members' privacy by:

> a. Intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person.
>
> b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and
>
> c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

206. Indeed, given the foreseeability of the harms inherent in data breaches and the ubiquitous nature of data breaches, Defendant was substantially certain that its failure to implement reasonable cybersecurity standards would lead to an invasion of Plaintiffs privacy.

207. Defendant knew that an ordinary person in Plaintiffs or Class Members' position would consider the exposure of their PII to be highly offensive and objectionable.

208. Defendant invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

209. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

210. Moreover, given that stolen PII is then publicized and traded on the dark web and through Telegram channels, Defendant knew or was substantially certain that its failure to implement reasonable cybersecurity safeguards would lead to the publication of Plaintiffs and the Class Members' PII to a large group of the public and/or to a large group of individuals who are in a special relationship with Plaintiffs and the proposed Class Members, in that those individuals are exactly the type of people that Plaintiffs and the Class Members have a special interest in ensuring their PII is kept confidential from given that those individuals are known identity thieves and fraudsters.

211. The conduct described above was at or directed at Plaintiffs and the Class Members.

212. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

213. In failing to protect Plaintiffs and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

THIRD COUNT - UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

214. Plaintiffs repeat and re-allege each and every factual allegation contained in the previous paragraphs 1 through 178.

215. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count, the third count listed in this Complaint.

216. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its clients and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

217. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

218. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

219. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

220. Defendant, however, failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

221. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

222. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

223. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

224. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit.

Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

225. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

226. Plaintiffs and Class Members have no adequate remedy at law.

227. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (I) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) 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 backed up 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.

228. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

229. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from

them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their 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 Plaintiffs and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members.

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to client data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach.

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs 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 Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members.

v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs 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 securing checks.

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all clients, with additional training to be provided as appropriate based upon the clients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members.

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

xiii. Requiring Defendant to implement a system of tests to assess its respective clients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing clients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information.

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 personal identifying 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

xvii. for a period of 5 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct.

F. Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiffs and the Class.

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law.

H. For an award of punitive damages, as allowable by law.

I. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees.

J. Pre- and post-judgment interest on any amounts awarded at the prevailing legal rate; and

K. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Classes, hereby demands a jury trial on all issues so triable.

Dated: March 18, 2026

Respectfully submitted,

/s/ Angelica Gentile

Angelica Gentile
Texas Bar No. 24112322
Shamis & Gentile, P.A.
540 Heights Blvd. Ste. 330B
Hoston, TX 77007
(305) 479-2299
agentile@shamisgentile.com

Leanna A. Loginov (*pro hac vice* forthcoming)
Shamis & Gentile, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
lloginov@shamisgentile.com

Counsel for Plaintiff and the Proposed Class Members