IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MOSANTHONY WILSON, individually and on behalf of all others similarly situated, *Plaintiff,* v. MONEYGRAM PAYMENT SYSTEMS, INC., *Defendant*.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Mosanthony Wilson ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his attorneys, brings this action against MoneyGram Payment Systems, Inc. ("Defendant") and alleges, upon his personal knowledge and as to his own actions and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Financial services providers that collect consumers' sensitive information, including their names, phone numbers, addresses, email addresses, dates of birth, financial account numbers, Social Security numbers and/or passport numbers ("Personally Identifiable Information" or "PII"), have a duty to the consumers to protect their valuable, sensitive information.

2. Defendant is an American interstate and international peer-to-peer payments and money transfer company that was acquired by the private equity firm Madison Dearborn Partners in 2023 for $1.8 billion. Defendant operates brick and mortar services desks as well as a mobile app to facilitate peer-to-peer payments or money transfers. As a corporation whose bread and

butter requires the gathering of highly sensitive consumer financial information, Defendant is well aware of the life-altering impact a data breach can wreak on the average MoneyGram customer or user.

3. Despite Defendant's status as a sophisticated financial services provider, Defendant failed to properly protect customers and users by investing in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive PII that customers entrusted to Defendant in order to effectuate peer-to-peer payments or money transfers. Between September 20 and 22, 2024, Defendant's failure to safeguard customer data resulted in a catastrophic, widespread data breach in which customer and user data was breached and exfiltrated (the "Data Breach").

4. The compromised data included consumer names, phone numbers, email addresses, and postal addresses, dates of birth, Social Security numbers, copies of government-issued identification documents such as driver's licenses, other identification documents such as utility bills, bank account numbers, MoneyGram Plus Rewards numbers, transaction information including dates and amounts of transactions, and criminal investigation information such as allegations of fraud.[1]

5. Defendant did not identify the data breach until September 27, 2024, nearly a week after the breach occurred. Defendant waited another week until October 7, 2024 to announce the breach publicly. As a result, MoneyGram users like Plaintiff had no knowledge that their information was at risk for more than two weeks, costing them valuable time during which they could have taken proactive measures to protect themselves and their data.

6. Following the Data Breach, reports circulated online that MoneyGram was breached through a social engineering attack on the company's internal help desk that allowed the

[1] https://www.moneygram.com/mgo/us/en/notification/notice/ (last accessed October 27, 2024).

threat actors to access MoneyGram's network using an employee's credentials and target employee information in the company's Windows Active Directory Services. [2]

7. Notably, Defendant has not announced how many individuals have been impacted by the data breach, and based on Plaintiff's experience, Defendant is not even able to identify whose information was stolen in the breach.

8. Despite the highly sensitive nature of the personal information Defendant collected, and the prevalence of data breaches impacting financial services, Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiff and the Class. The Data Breach itself and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, and the sensitive nature of the impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

9. Defendant did not identify the data breach until September 27, 2024, nearly a week after the breach occurred. Defendant knew or should have known of the serious risk of harm caused by a data breach, including the importance of acting swiftly to protect PII. Yet, Defendant waited another week until October 7, 2024 to announce the breach publicly.

10. Defendant's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited Defendant's security vulnerabilities could monetize, misuse, and/or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect

[2] https://www.bleepingcomputer.com/news/security/moneygram-no-evidence-ransomware-is-behind-recent-cyberattack/ (last accessed October 27, 2024).

their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated even beyond the Data Breach itself.

11. Plaintiff and Class members had a reasonable expectation and understanding that Defendant would adopt adequate data security safeguards to protect their PII.

12. However, Defendant failed to: take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data to prevent the Data Breach from occurring; to disclose to customers or users the material fact that it lacked appropriate data systems and security practices to secure PII; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Because of Defendant's failures, Plaintiff and Class members suffered substantial harm and injury.

13. As a direct result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third parties for the purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendant's customers and users.

14. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

15. Plaintiff and Class members suffered injuries as a result of Defendant's conduct, including, but not limited to: loss of diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct, and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to 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 its PII. These risks will remain for the lifetimes of Plaintiff and the Class.

16. Plaintiff brings this action individually and on behalf of the Class, seeking relief including, but not limited to, compensatory damages, statutory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. PARTIES

17. Plaintiff has been at all relevant times a citizen and resident of San Diego, California.

18. Defendant is a private corporation wholly owned by Madison Dearborn Partners. Defendant is incorporated under the laws of Delaware and maintains a headquarters at 2828 N. Harwood, 15th Floor Dallas, TX.

III. JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of costs and

interest. Moreover, because of the scope of Defendant's business, the Class likely includes individuals from all over the United States, and there are more than 100 putative Class members.

20. Venue is proper in this judicial district under 28 U.S.C. § 1391 because Defendant is headquartered and transacts substantial business in this district, and because a substantial portion of the events giving rise to Plaintiff's claims occurred here.

21. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Dallas, Texas.

IV. FACTUAL BACKGROUND

A. Defendant Collects Highly Sensitive Financial Information from Customers and Users.

22. MoneyGram is one of the largest money transfer services companies in the world and operates in more than 200 countries and territories across more than 430,000 locations.[3]

23. In order to effectuate peer-to-peer payments or money transfers, MoneyGram collects sensitive PII and financial information including, but not limited to, names, phone numbers, email addresses, and postal addresses, dates of birth, Social Security numbers, copies of government-issued identification documents such as driver's licenses, other identification documents such as utility bills, and bank account numbers.

24. As a result, Defendant hosts a large repository of sensitive personal information maintained for its customers and received from customers and users, including Plaintiff and the Class.

B. Defendant Failed to Adequately Protect Customer and User Data, Resulting in the Breach.

[3] https://www.cybersecuritydive.com/news/moneygram-cyberattack-sensitive-data/729342 (last accessed October 27, 2024).

25. From September 20 to 22, 2024, a malicious actor gained unauthorized access to Defendant's company data systems and acquired personal information of consumers including names, phone numbers, email addresses, and postal addresses, dates of birth, Social Security numbers, copies of government-issued identification documents such as driver's licenses, other identification documents such as utility bills, bank account numbers, MoneyGram Plus Rewards numbers, transaction information including dates and amounts of transactions, and criminal investigation information such as allegations of fraud.[4]

26. Defendant did not identify the data breach until September 27, 2024, nearly a week after the breach occurred. Defendant knew or should have known of the serious risk of harm caused by a data breach, including the importance of acting swiftly to protect PII. Yet, Defendant waited another week until October 7, 2024 to announce the breach publicly.

27. Defendant has not yet announced how many people have been impacted, and as revealed by Plaintiff's experience described in Section IV (F) *infra*, is unable to even identify ***whose*** data has been impacted.

28. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

29. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

30. Additionally, MoneyGram was aware of the importance of protecting consumers'

[4] https://www.moneygram.com/mgo/us/en/notification/notice/ (last accessed October 27, 2024).

financial data because it previously paid $125 million to settle allegations that the company failed to take steps required under a 2009 Federal Trade Commission order to crack down on fraudulent money transfers that cost U.S. consumers millions of dollars.[5]

C. Defendant Failed to Take Adequate Actions Prior to and Following the Data Breach.

31. Defendant has an obligation to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Defendant's obligations are derived from: (1) government regulations and laws, including FTC rules; (2) industry standards; and (3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided—and Defendant obtained—their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

32. Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

33. Cyber-attacks and ransomware attacks are frequently used to target companies or large entities due to the volume of sensitive data that they collect, maintain, and store.[6]

34. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and network files containing PII.

35. Despite widespread industry warnings, Defendant failed to implement and use reasonable security procedures and practices to protect Plaintiff's and similarly situated individuals' sensitive PII.

---

[5] https://www.ftc.gov/news-events/news/press-releases/2018/11/moneygram-agrees-pay-125-million-settle-allegations-company-violated-ftcs-2009-order-breached-2012 (last accessed October 27, 2024).

[6] Charles Griffiths, *The Latest 2024 Cyber Crime Statistics (updated July 2024)*, AAG (Jan. 7, 2024), available at https://aag-it.com/the-latest-cyber-crime-statistics/ (last accessed October 27, 2024).

36. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed unauthorized actors to access sensitive PII.

37. The Data Breach highlights the inadequacies inherent in Defendant's network monitoring procedures and security training protocols. If Defendant had properly monitored its cybersecurity systems and implemented a sufficient training protocol for its employees, it would have prevented the Data Breach, detected the Data Breach sooner, and/or have prevented the hackers from accessing PII.

38. Defendant's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

39. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

40. Defendant's failures are three-fold. First, Defendant failed to timely secure its computer systems to protect customers' and users' PII and sensitive financial information. Defendant allowed unauthorized actors to access and exfiltrate highly sensitive PII and other financial information from an unknown number of MoneyGram users and customers without detection.

41. Second, Defendant failed to timely notify affected individuals, including Plaintiff and Class members, that their highly sensitive PII had been accessed by unauthorized third parties. Despite the breach beginning on September 20, 2024, Defendant failed to take any action until October 7, 2024.

42. Third, Defendant made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Although Defendant offered victims 24

months of credit monitoring, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long into the future. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

43. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and to timely notify Plaintiff and the Class that their PII had been accessed due to Defendant's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII for an unknown amount of time before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats.

44. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors and lead to considerable costs to consumers. According to Statista, during the first quarter of 2023 alone, more than six million data records were exposed worldwide through data breaches.[7] Indeed, cybercrime is slated to cost the world $10.5 trillion annually by 2025.[8]

45. Identity theft is the most common consequence of data breaches to consumers. A 2021 report concluded that more than half of all data breaches resulted in identity theft, including unauthorized access to a victim's financial accounts, opening new accounts in the victim's name,

[7] https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (last accessed October 27, 2024).

[8] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020), available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (last accessed October 27, 2024).

and using a victim's personal information for other fraudulent activities.[9]

46. As a result, PII is an invaluable commodity and the most frequent target of hackers.[10] Numerous sources cite dark web pricing for personal information, such as name, date of birth, and Social Security number, ranging from $40 to $200.[11]

47. Many tend to minimize the value of certain categories of PII, such as names, birthdates, addresses, and phone numbers. However, security experts agree that "[i]f you have someone's name and address, that is still valuable."[12] At the end of the day, "the more info you have, the more it is worth."[13]

48. Thefts of Social Security numbers present an even greater risk to consumers. Indeed, data breaches involving Social Security numbers are "incredibly alarming" because "[u]nlike a credit card number which can be changed, Social Security numbers . . . are hard to change, or cannot be changed."[14]

49. Even if victims whose Social Security numbers have been compromised are able to change their Social Security numbers, the new number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

---

[9] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed October 27, 2024).

[10] *Id*.

[11] *Id*.

[12] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), available at https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html (last accessed October 27, 2024).

[13] *Id.*

[14] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015), available at https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed October 27, 2024).

old bad information is quickly inherited into the new Social Security number."[15]

50. According to the FTC, in 2021, around 20% of Americans were victims of identity theft, indicating that most Americans have either been a victim of identity theft or know someone who has.[16]

51. The fraudulent activity resulting from Defendant's Data Breach may not come to light for years, as there may be a time lag between when Plaintiff's and Class members' PII was stolen and when it is used, meaning there may be a delay between when the harm occurs versus when it is discovered.[17]

52. Beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.[18]

53. Despite the prevalence of public announcements of data breach and data security compromises and the risks posed by compromises of PII, Defendant failed to take proper action to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were foreseeable and directly caused by Defendant's failure to implement or

---

[15] *Id*.

[16] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission (Feb. 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last accessed October 27, 2024).

[17] *Report to Congressional Requesters*, Government Accountability Office, at 29 (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last accessed October 25, 2024).

[18] *New Study by Identity Theft Resource Center Explores the Non-Economic Negative Impacts Caused by Identity Theft*, Identity Theft Resource Center (Oct. 18, 2018), available at https://www.idtheftcenter.org/post/new-study-by-identity-theft-resource-center-explores-the-non-economic-negative-impacts-caused-by-identity-theft/#:~:text=Due%20to%20their%20identity%20theft,at%20school%20(eight%20percent) (last accessed October 27, 2024).

maintain adequate data security measures for its customers and users.

E. Defendant's Conduct Violated the FTC Act & Industry Standards for Safeguarding Customers and Users' PII.

54. The FTC rules, regulations, and guidelines obligate businesses to protect PII from unauthorized access or disclosure by unauthorized persons.

55. At all relevant times, Defendant was fully aware of its obligation to protect its customers' and users' PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII.

56. Defendant was also aware of the significant consequences of its failure to protect the PII of its customers and users and knew that this data, if hacked, would injure individuals, including Plaintiff and Class members.

57. Defendant failed to comply with FTC rules, regulations, and guidelines and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of customers' and users' PII;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its customers' and users' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures, and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former customers or users' PII.

58. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and customers or users of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

F. Plaintiff's Experience

59. Plaintiff has used MoneyGram to transfer money on a regular basis for approximately three years.

60. Plaintiff typically goes into a Wal-Mart twice a month to complete his transfers through MoneyGram.

61. Plaintiff learned of the Data Breach sometime around October 10, 2024, when he saw an article about the Data Breach on Google News.

62. On October 22, 2024, Plaintiff called Defendant's Data Breach hotline at (833) 918-1122 and inquired whether he was implicated in the Data Breach. The hotline could not answer whether Plaintiff had been impacted by the Data Breach, but they offered to enroll Plaintiff in

complimentary credit monitoring.

63. Plaintiff reasonably believes that he was impacted by the Data Breach because he frequently uses MoneyGram services and Defendant offered him the credit monitoring services it is providing to Data Breach victims.

64. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff has spent valuable time dealing with the Data Breach, time Plaintiff otherwise would have spent on other activities, including work and/or recreation.

65. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft; and (d) loss of benefit of the bargain.

66. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

67. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Nationwide Class defined as:

> **All persons in the United States whose PII was accessed in the Data Breach announced by Defendant on October 7, 2024 (the "Nationwide Class").**

68. Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the Class definition after conducting discovery.

69. In addition, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a California Subclass defined as:

> **All persons who are residents of the State of California whose PII was accessed in the Data Breach announced by Defendant on January 8, 2024 (the "California Subclass").**

70. Excluded from the California Subclass are Defendant and its executives and officers.

71. The Nationwide Class and the California Subclass are collectively referred to herein as the "Class."

72. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that at least thousands of individuals' PII were affected by the Data Breach. The members of the Class will be identified through information and records in Defendant's possession, custody, and control.

73. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct;

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief, and/or other remedies and, if so, the nature of any such relief.

74. **Typicality**: Plaintiff's claims are typical of the claims of the Class because Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The actions and omissions that gave rise to Plaintiff's claims are the same that gave rise to the claims of every other Class member because Plaintiff and each Class member had their sensitive PII compromised in the Data Breach due to Defendant's misconduct, and there are no defenses that are unique to Plaintiff.

75. **Adequacy**: Plaintiff is an adequate representative because his interests do not

conflict with the interests of the Class that he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

76. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on Defendant's records.

77. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

(On Behalf of Plaintiff and the Class)

78. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

79. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

80. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendant collected.

81. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

82. Defendant owed a duty of care to Plaintiff and the Class because it was a foreseeable and probable victim of any inadequate data security practices.

83. Defendant solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

84. Defendant knew or should have known it inadequately safeguarded this information.

85. Defendant knew that a breach of its systems would inflict significant monetary damages upon Plaintiff and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

86. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

87. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Defendant's misconduct included failing to: (1) secure its systems, servers,

and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement safeguards, policies, and procedures necessary to prevent this type of data breach.

88. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

89. Defendant breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

90. Defendant breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

91. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

92. Defendant breached the duties it owed to Plaintiff and the Class by failing to disclose timely and accurately to Plaintiff and Class members that their PII had been improperly acquired or accessed.

93. Defendant breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about October 7, 2024.

94. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before

the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

97. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

98. Defendant violated the FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of the Data Breach, and the exposure of Plaintiff's and Class members' sensitive PII.

99. Defendant's violations of the FTC rules and other applicable standards constitute negligence *per se*.

100. Plaintiff and the Class are within the category of persons the FTC Act was intended to protect.

101. The harm that occurred as a result of the Data Breach described herein is the type of harm the FTC Act was intended to guard against.

102. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III - BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Class)

103. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

104. When Plaintiff and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' PII, comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII, and to timely notify them in the event of a data breach.

105. Defendant solicited and invited Plaintiff and Class Members to provide their PII as in order to effectuate payment services. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

106. Implicit in the agreement between Plaintiff and Class Members and Defendant was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard Plaintiff's and Class Members' PII; (c) prevent unauthorized access and/or disclosure of Plaintiff's and Class Members' PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII; (e) reasonably safeguard and protect the PII of Plaintiff's and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiff's and Class Members' PII under conditions that kept such information secure and confidential.

107. Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect

Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

108. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

109. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

110. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII and by failing to provide them with timely and accurate notice of the Data Breach.

111. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Loss of money due to fraudulent withdrawals and fraudulent transfers from their financial accounts;

d. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling

and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

j. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

k. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

COUNT IV - VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

(On Behalf of Plaintiff and the California Subclass")

112. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

113. Defendant violated California Civil Code § 1798.150(a) of the CCPA by failing to

implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the California Subclass. As a direct and proximate result, Plaintiff's unencrypted and unredacted PII was subject to unauthorized access and exfiltration and theft.

114. Defendant is a "business" under the meaning of California Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

115. Plaintiff seeks injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's PII. Plaintiff has an ongoing interest in ensuring that his PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

116. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

117. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

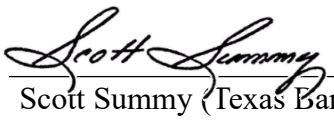
118. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the proposed Class, respectfully requests a trial by jury as to all matters so triable.

Dated: November 4, 2024

Respectfully submitted,

By: 

Scott Summy (Texas Bar No. 19507500)
BARON & BUDD, P.C.
3102 Oak Lawn Avenue, Suite 1100
Dallas, TX 75219-4281
Telephone: (214) 521-3605
Fax: (214) 279-9915
ssummy@baronbudd.com

Elizabeth A. Fegan
Megan E. Shannon
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com