UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CARNEL FAULKNER, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. MONEYGRAM PAYMENT SYSTEMS, INC. and MONEYGRAM INTERNATIONAL, INC., Defendants.	CIVIL ACTION NO. 3:24-CV-2557-S **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Carnel Faulker individually and on behalf of all others similarly situated, ("**Plaintiff**") brings this Action against Defendants MoneyGram Payment Systems, Inc. ("**MPSI**") and MoneyGram International, Inc. ("**MGI**") (collectively, "**MoneyGram**" or "**Defendants**"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth below, after a reasonable opportunity for discovery.

INTRODUCTION

1. MoneyGram is a leading global money transfer and payment services company, offering services in more than 200 countries and territories, operating "one of the largest cash distribution services in the world."[1] As of 2024, MoneyGram serves over 150 million customers and provides its MoneyGram platform to purportedly "enable seamless and secure transfers around

[1] *About MoneyGram* (N.D.). MoneyGram, from https://corporate.moneygram.com/about-us/#Leadership (Last visited Nov. 25, 2024).

the world."[2] Plaintiff and millions of other consumers entrusted MoneyGram with their personal data when they registered for accounts or each time they transferred money through MoneyGram's website and mobile application platforms (hereinafter, "**Platform**"), providing their names, contact information, social security numbers, government-issued identification numbers, bank account numbers, and prior transaction details and history.[3] As stated in its privacy policy, MoneyGram itself recognizes the heavy burden of protection and security that it bears when collecting and storing this data.[4] MoneyGram further represents that it "use[s] a variety of robust physical, technical, organizational, and administrative safeguards to protect [customers'] personal data from unauthorized access, loss or alteration."[5] MoneyGram touts its purported dedication to strong security by making the following advertising claims for its devices and services, including but not limited to, the following:

- "We Lead the Industry in Protecting Customers."[6]
- "MoneyGram works diligently to prevent its systems from being used to perpetrate any unlawful activity."[7]
- "We are committed to safeguarding the privacy of your Personal Information."[8]
- "We use the appropriate organization, technical and administrative measures to maintain the security of your Personal Information and to protect against the destruction, loss,

[2] *BamSEC*. (2024, February 23). MoneyGram, from https://www.bamsec.com/filing/127393123000039?cik=1273931 (Last visited Nov. 25, 2024).
[3] *Consumer Data Notice* (2024, Oct. 7), MoneyGram, from https://www.moneygram.com/intl/us-notice
[4] *Global Privacy Notice*. (2023). MoneyGram, from https://www.moneygram.com/intl/privacy-center/global-privacy-notice (Last visited Nov. 25, 2024).
[5] *Id.*
[6] *Compliance*. (N.D.). MoneyGram, from https://corporate.moneygram.com/compliance/?_ga=2.240501386.802156005.1728503421-438024125.1728503421 (Last visited Nov. 25, 2024).
[7] *Id.*
[8] *Global Privacy Notice.* (Apr. 1, 2022). MoneyGram, available at https://www.tbcbank.ge/web/documents/10184/666084/Updated-MoneyGram-Global-Consumer-Notice-Privacy-ENG.pdf/2ac2cb71-9efc-4ca0-a988-366fdcafddd2 (Last visited Nov. 25, 2024)

alternation, unauthorized disclosure, or access to Personal Information under our control."[9]

- "We also take preventive measures to restrict access to Personal Information to only those who have need to know . . . All who have access to, or are associated with, the processing of Personal Information are contractually obligated to respect the confidentiality of your Personal Information."[10]

2. MoneyGram's representations of strong security have proved false and misleading—MoneyGram failed to safeguard the sensitive personal identifying information of millions of its consumers and failed to implement necessary security measures to prevent this information from being stolen.

PARTIES

Plaintiff Carnel Faulker

3. Plaintiff Carnel Faulker is a citizen and resident of the State of California who had his personal identifiable information and personal financial information ("personal identifiable information" and "personal financial information" are collectively "**Private Information**") exfiltrated and compromised in the data breach announced by MPSI on October 7, 2024.

4. Plaintiff has regularly used MoneyGram for years, first using it to pay rent 8-10 years ago. To transfer money through the Platform, Plaintiff was required to provide two forms of identification, which included his government-issued driver's license number, and to fill out a form which listed his bank account information and his social security number. Plaintiff last transferred funds through the Platform during or around autumn of 2023. In total, Plaintiff was required to provide MoneyGram with his name, contact information, social security number, government-issued identification number, and bank account numbers, among other information.

5. In making his decision to utilize the Platform to transfer money, Plaintiff reasonably expected that MoneyGram would safeguard his Private Information and destroy it after completing

[9] *Id.*
[10] *Id.*

Plaintiff's request to send/receive money. Plaintiff would not have used the Platform for money transfers, if he knew that the sensitive information MoneyGram collected would be at risk. Plaintiff has suffered damages and remains at significant risk now that his Private Information has been leaked online and/or otherwise compromised.

6. As a result of this data breach, Plaintiff has spent substantial time in attempt to mitigate damages caused by this data breach, including monitoring all of his accounts and financial activity. The time spent dealing with Defendants' data breach is time Plaintiff otherwise would have spent it on other activities such as work and/or recreation. Plaintiff anticipates taking additional time-consuming and necessary steps to help mitigate the harm caused by the data breach, including continuously reviewing his accounts for unauthorized activity.

Defendant MoneyGram Payment Systems, Inc.

7. Defendant MoneyGram Payment Systems, Inc. ("MPSI") is a Delaware corporation with its principal place of business and headquarters located at 2828 N. Harwood St., #15, Dallas, Texas, from where its officers direct, control, and coordinate the corporation's activities.

8. MPSI offers and sells various money transfer products and services to consumers, including but not limited to peer-to-peer payments, international wire transfers, money orders, and digital wallets.

Defendant MoneyGram International, Inc.

9. Defendant MoneyGram Payment Systems, Inc. ("MGI") is a Delaware corporation with its principal place of business located at 2828 N. Harwood St., #15, Dallas, Texas, from where its officers direct, control, and coordinate the corporation's activities.

10. There exists, and at all relevant times existed, a unity of ownership between MPSI and MGI and their agents such that any individuality or separateness between them has ceased and each of them is the alter ego of the others. Adherence to the fiction of the separate existence of MGI and MPSI would under the circumstances set forth in this complaint promote injustice.

11. For example, there is substantial overlap among the senior management of MGI and MPSI, and the bulk of both MGI's and MPSI's legal and compliance operations are managed by MoneyGram's senior management in Dallas, Texas, where eight out of sixteen executive officers oversee the companies' global operations, including Chief Executive Officer, Chief Financial Officer, Chief Marketing Officer, Chief Compliance Officer, and Chief Data and Analytics Officer, along with several other executive officers. [11] Moreover, MGI represents in its Global Privacy Notice that it conducts its business primarily through MPSI, which is its wholly owned subsidiary.[12]

12. At all relevant times, through the data breach, both entities also shared the CEO, William Alexander Holmes, who resided (and still resides) in Dallas Texas from where he directed and managed MoneyGram's activities. The new CEO and global director of both entities is Anthony Soohoo, who also presently resides in Dallas Texas, and directs MoneyGram's activities from Texas. Likewise, the entities share a Chief Technology Officer, who has been and presently resides and directs operations of MoneyGram entities from Dallas Texas.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendants. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367. Furthermore, the affected victims of the data breach – the Class Members – reside nationwide.

[11] MoneyGram entities were previously headquartered in Minneapolis, Minnesota, but the principal place of business was moved to Texas in or around 2010, from where the bulk of both MGI's and MPSI's legal and compliance operations are managed by the corporate officers in Texas. The remaining executive officers reside in Minnesota, Colorado, New York, Chicago, and D.C.; however, the principal place of business of the two entities remains in Texas.
[12] *Supra,* note 4.

14. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims occurred in this District: MoneyGram is registered in Texas and headquartered in this District, MoneyGram gains revenue and profits from doing business in this District, consumers sign up for MoneyGram accounts, transfer money through the Platform and provide MoneyGram with their Private Information in this District, Class members were affected by the breach from MoneyGram's actions and inactions directed from this District, MoneyGram has a corporate office in this District, and MoneyGram employs corporate officers in this District, from where MoneyGram's officers direct the corporate activities for both entities.

15. MoneyGram is subject to personal jurisdiction in Texas becauseit conducts substantial business in this judicial district, both MoneyGram entities' principal place of business are located within this State, where the entities' corporate officers are also located including their CEO and CTO, as well as their other top management. MoneyGram conducts business and has purposefully availed itself of the benefits and protections of Texas by continuously and systematically conducting substantial business in this judicial district including by directing advertising and marketing materials from the State of Texas.

FACTUAL ALLEGATIONS

16. MoneyGram is a leading global money transfer and payment services company. Founded in 1940, MoneyGram has grown to be one of the largest money transfer providers worldwide.[13]

17. MoneyGram offers a wide range of financial services, including domestic and international money transfers, bill payments and mobile wallet transactions. MoneyGram serves over 150 million customers in more than 200 countries and territories, with a network of approximately 347,000 agent locations globally. The company utilizes various brands under its corporate umbrella, including MoneyGram, WalMart2World, and MoneyGram Online.[14]

[13] *Supra,* note 1
[14] *Id.*

18. MoneyGram collects and processes the personal data of millions of consumers, including sensitive personal and financial information. The information collected and stored by MoneyGram includes, but is not limited to, "***names, contact information (such as phone numbers, email 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 (such as dates and amounts of transactions)***."[15] MoneyGram collected this Private Information by requiring users to complete account registration and verify their identities to send funds through Platform and continues to collect and store this Private Information when users transfer money.

19. MoneyGram holds itself as a trustworthy company, which recognized and values the customers' privacy and personal information and has repeatedly assured its customers that it is "committed" to data security.[16]

20. MoneyGram's privacy policy and online advertisements clearly and unequivocally state that any personal information provided to MoneyGram will remain secure and protected, driving the point home that *MoneyGram wants customers to believe their personal information will be safeguarded*:

> **At MoneyGram ("we," "us" and "our" will refer to the specific company with which you interact, and "MoneyGram" will refer to the MoneyGram group of companies), we respect your privacy and are committed to handling your personal data responsibly and in accordance with applicable laws.[17]**

21. Plaintiff and other similarly situated consumers relied to their detriment on MoneyGram's uniform representations and omissions regarding data security, including MoneyGram's failure to alert customers that its security protections were inadequate, and that

[15] *Supra,* note 3
[16] *Supra,* note 8
[17] *Supra,* note 4

MoneyGram would forever store Plaintiff's and customers' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach. Given that the use of MoneyGram's services requires an exchange of highly sensitive information such as social security information, bank accounts, state-issued driver license information and other sensitive data, Plaintiff and other Class Members expect MoneyGram to adhere to their prominent promises that the information would be safeguarded.

22. Had MoneyGram disclosed to Plaintiff and its other customers that its data systems were not secure and were vulnerable to attack, Plaintiff would not have utilized MoneyGram's services.

23. Plaintiff and other similarly situated consumers trusted MoneyGram with their sensitive and valuable Private Information. MoneyGram did not need to store this Private Information at all. Once identities are verified, as Plaintiff was required to do *each time he transferred funds*, MoneyGram could delete government identification numbers. Instead, MoneyGram retains personal information to mine it for value, to increase its profits, to gather additional information regarding its customers, and to track its customers and their behaviors.

24. MoneyGram knew or should have known that Plaintiff and Class Members would reasonably rely upon and trust its promises regarding security and safety of its data and systems.

25. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other customers' Private Information, and utterly failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, MoneyGram caused harm to Plaintiff and consumers.

THE DATA BREACH

26. At all material times, MoneyGram failed to maintain proper security measures despite its promises of safety and security to consumers and despite its substantial financial resources and ability to do so.

27. On September 27, 2024, MoneyGram detected unauthorized access to its systems

which started nearly a week prior between September 20-22.[18] MoneyGram revealed that attackers had gained access through a social engineering attack on MoneyGram's IT help desk.[19] A hacker impersonated an employee, and easily gained access to the company's network through the help of MoneyGram's other employees.

28. MoneyGram publicly disclosed the data breach on October 7, 2024, approximately ten days after detecting unauthorized access.[20] It confirmed that sensitive customer information had been compromised, including ***names, contact details, dates of birth, Social Security numbers, copies of government-issued IDs, bank account information, and even MoneyGram transaction details.***[21]

29. In its statement, MoneyGram does not disclose how many customers' Private Information was breached, leaving consumers to speculate whether it is likely that their Private Information has been compromised and without clear instruction on what they can do to protect themselves and mitigate their losses now that their PII has been exposed. However, MoneyGram has more than 150 million customers, and therefore, it is highly likely that millions of people have been affected nationwide.

30. After the massive data breach, MoneyGram's remedy – instead of providing consumers with recovery and clear instructions if they were affected and how they could protect

---

[18] Grieg, Jonathan (Nov. 25, 2024). *MoneyGram Says Customer Information Stolen During September Attack*, THERECORD, from https://therecord.media/moneygram-says-customer-information-stolen (Last visited Nov. 25, 2024); Ardrey, Taylor (Nov. 25, 2024). *MoneyGram Announces Hack: Customer Data Such as Social Security Numbers, Bank Accounts Impacted,* AOL.com [via USA TODAY], from https://www.aol.com/moneygram-announces-hack-customer-data-131627863.html (Last visited Nov. 25, 2024).

[19] Uliss, Ryan, *MoneyGram Confirms its Recent Cyberattack Exposed Sensitive Customer Data,* NATIONALCIOREVIEW, from https://nationalcioreview.com/articles-insights/extra-bytes/moneygram-confirms-its-recent-cyberattack-exposed-sensitive-customer-data/ (Last visited Nov. 25, 2024).

[20] Binder, Matt, *MoneyGram Confirms Hack: Social Security Numbers, Driver's Licenses, and Other Customer Data Have Leaked,* MASHABLE, from https://mashable.com/article/moneygram-data-breach (Last visited Nov. 25, 2024).

[21] *Supra,* Note 3

themselves – was apparently to simply fire their CEO, Alex Holmes. However, this is not enough to remedy the Data Breach.

MoneyGram Failed to Comply with FTC Guidelines, Follow Industry Standards, & Implement Basic Security Measures

31. MoneyGram was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

32. The FTC has promulgated numerous guides for businesses which 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.

33. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

34. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

[22]Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business /. (Last accessed November 8, 2024).
[23] *Id.*

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.

35. Furthermore, FTC requires that the companies like MoneyGram conduct risk assessments, implement and periodically review access control, encrypt customer information, implement multi-factor authentication for anyone accessing customer information within their systems, dispose of customer information securely, maintain a log of authorized users' activity and keep an eye out of unauthorized access, train employees regarding security awareness, conduct audits, penetration testing, and system wide scans regularly to test for publicly known security vulnerabilities – all of which if had been properly implemented would have allowed MoneyGram to prevent this Data Breach.

36. MoneyGram failed to properly implement basic data security practices, allowing for this attack to occur, victimizing millions of people – by failing to adhere to many of the FTC set protocols and allowing access to a hacker impersonating an employee. MoneyGram should have followed security steps, verified the employee's information, obtained the impersonated employees multiple forms of identifications through secure means (including a video verification of employee impersonator), used other secure methods such as biometric data verification, conducted knowledge-based and credit score identification, and utilized a multifactor authentication before allowing the impersonator access to highly sensitive data. Had MoneyGram maintained the proper employee verification protocols, trained its employees to recognize the social engineering scams, deleted and encrypted customer data in its possession, and regularly conducted audits to ensure its vulnerabilities and training, it would have prevented the Data Breach.

37. MoneyGram failed to properly implement the FTC guidelines by allowing access to the threat actor to the most sensitive data (such as social security information, bank account information) after the transactions had been completed – the data that should have been deleted in the first place.

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

39. Furthermore, companies like MoneyGram that have access to highly sensitive data such as social security numbers and even bank account information of individuals must comply with the industries' best practices of ensuring employees' security compliance, which require implementing thorough analyses, regular audits and risk assessments, penetration testing (which includes testing employees' knowledge on social engineering attempts and access), proactively identifying and addressing weaknesses in the company's systems, clear policies and procedures, and most importantly implementing strong access controls and authentication measures (such as biometric authentication, encryption, multifactor authentication).

40. Given the rise of social engineering scams, responsible companies implement identity verification protocols for employees and customers through: (a) ID document authentication (like submission of passports, driver licenses); (b) match the submitted documents with the biometrics and liveness checks; (c) conduct face matching; and (d) conduct knowledge-base authentication which consists of series of personal questions, the answers to which would be known only to the employee/holder. MoneyGram, however, has not implemented these protocols resulting in its employee/imposter gaining access to a large amount of consumers' sensitive data.

IMPACT OF DATA BREACH ON CONSUMERS

41. Plaintiff and the Class have suffered actual harm as a result of MoneyGram's conduct. MoneyGram failed to institute adequate security measures and neglected system vulnerabilities that led to the data breach. This breach allowed a hacker to access the Private Information, including names, contact information, dates of birth, Social Security numbers, government-issued identification documents, bank account numbers, and transaction information, for Plaintiff and the Class. This Private Information was accessed by a person who engaged in social engineering with the purpose of acquiring this information. Upon information and belief, the social engineer who accessed MoneyGram's systems is a criminal, and intends to either sell,

trade, or otherwise operationalize the stolen information to perpetuate scams, identity theft, and further social engineering schemes. Now that the Private Information is in the hands of a nefarious individual, it will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[24]

42. PII is a valuable property right.[25] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[26] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[27] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

43. Plaintiff and other Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

44. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

---

[24] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf. (Last visited April 1, 2024).

[25] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_%20The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...") (Last accessed November 8, 2024).

[26] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (Last accessed November 8, 2024).

[27] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (Last accessed November 8, 2024).

45. As a result of its real value, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. The information exposed in the Data Breach can thus be aggregated, becoming more valuable to thieves and more damaging to victims.

46. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[28] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches.[29]

47. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[30]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

49. Plaintiff 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

---

[28] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), accessible at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[29] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), accessible at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[30] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1

suitable identity theft protection and credit monitoring services, and pay to procure them.

50. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of MoneyGram's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

51. MoneyGram fully understands the market value of data privacy – so much so that it dedicates substantial portions of its website promising users that "protecting customers is a priority, reminding users that its services are "secure. Furthermore, prior to any individual using MoneyGram's services, MoneyGram again reiterates in its disclosures that it "limit[s] personal information access to only employees, agents, and representatives who need to know [such information]." Contrary to its explicit promises and assurances, MoneyGram failed to maintain reasonable and adequate data security measures, and Plaintiff's and Class Members' PII has been and is now in the hands of unauthorized criminals.

Digital Phishing Scams

52. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[31]

53. Since the data breach, Plaintiff has experienced an increase in text messages from unknown numbers with embedded links. Given the perpetrator's willingness to engage in social engineering scams, it comes as no surprise that Plaintiff's and Class Members' information is now being used to conduct further scams.

54. MoneyGram's customers are now more likely to become victims of digital phishing

[31] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last visited April 1, 2024).

scams because of the released personal information.

SIM-Swap

55. The exfiltration of data can also lead to SIM-swap attacks against the Class.[9] A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

56. MoneyGram's customers are now more likely to become victims of SIM Swap attacks because of the released personal information.

Loss of Time

57. As a result of this data breach, Plaintiff and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach.

58. Plaintiff, in great distress, is attempting to change his passwords and associated accounts which may be connected to various pieces of stolen Private Information. Plaintiff has been monitoring his credit activity, now living in fear and apprehension of further attacks.

Overpayment for Platform Fees

59. Plaintiff and the Class would not have utilized the Platform if they knew that doing so would result in their Private Information being compromised and exfiltrated. Thus, they overpaid the associated fees on their money transfer transactions based on how the Platform was represented compared to what they received.

Threat of Identity Theft

60. As a direct and proximate result of MoneyGram's breach of confidence, and failure to protect the Private Information, Plaintiff and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and

confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. MoneyGram, through its misconduct, has enabled numerous bad actors to sell and profit off of Prive Information that belongs to Plaintiff and the Class.

61. But for MoneyGram's unlawful conduct, scammers would not have access to Plaintiff's and the Class Members' contact information. MoneyGram's unlawful conduct has directly and proximately resulted in widespread digital attacks against Plaintiff and the Class.

Out of Pocket Costs

62. Plaintiff is now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending out of pocket expenses to pay for these services.

63. MoneyGram also used Plaintiff's Private Information for profit and continued to use Plaintiff's Private Information to target Plaintiff, and share his information with various third parties, or to improve its marketing to other third parties for MoneyGram's own benefit.

Threat of Financial Fraud

64. The Data Breach has significantly increased the risk of financial fraud for affected customers. With access to sensitive financial information such as bank account numbers, transaction details, and MoneyGram's own loyalty program numbers, cybercriminals now have the tools to conduct unauthorized transactions or engage in financial identity theft.

65. Customers whose information was compromised in the Data Breach face an elevated risk of unauthorized money transfers or account takeovers and was the proximate consequence of MoneyGram's failure to secure its customers' Private Information.

No Adequate Remedy at Law

66. No adequate remedy at law. Plaintiff and the Class are entitled to equitable relief as no adequate remedy at law exists.

i. MoneyGram has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

ii. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendants' misrepresentations regarding privacy and security of information and also to implement the necessary security measures to protect the information that may later be in MoneyGram's possession;

iii. The equitable relief under the UCL also creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendants' services). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims;

iv. MoneyGram has not disclosed full details surrounding its security failures and exactly how the imposter gained access to the data, nor did MoneyGram implement any measures to ensure that the PII in Defendants' possession will be deleted. Therefore, Injunctive relief would ensure and provide Plaintiff and the public with ability to control the access to their information, and limit their PII exposure;

v. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, in the absence of completed discovery regarding class certification and merits, forcing an election of remedies at the initial pleadings stage is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

Summary of Actual Economic and Noneconomic Damages

67. In sum, Plaintiff and similarly situated consumers were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information;

iii. Loss of value of their Private Information;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. MoneyGram's retention of profits attributable to Plaintiff's and other customers' Private Information that MoneyGram failed to adequately protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed to;

vii. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments of MoneyGram's products and/or services which Plaintiff purchased;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

CLASS ACTION ALLEGATIONS

68. Pursuant to Federal Rules 23(a), (b)(2), 23(b)(3), and/or (c)(4), as applicable, Plaintiff seeks certification of the following nationwide class ("Nationwide Class" or the "Class"):

> All persons residing in the United States and whose Private Information was accessed, compromised, or stolen in the data breach announced by MoneyGram on October 7, 2024.

69. Pursuant to Federal Rules 23(a), (b)(2), 23(b)(3), and/or (c)(4), as applicable, Plaintiff seeks certification of the following nationwide class ("California Subclass"):

> All persons residing in California and whose Private Information was accessed, compromised, or stolen in the data breach announced by MoneyGram on October 7, 2024." (the "**California Subclass**").

70. This class definitions may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

71. The Class is comprised of millions of consumers throughout the United States and the state of California. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

72. There is a well-defined community of interest in the questions of law and fact involved and affecting the parties to be represented. The Class was exposed to the same common and uniform false and misleading representations and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

b. Whether Defendants' conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

c. Whether Defendants' advertising as to its security practices is untrue or misleading within the meaning of Business and Professions Code section 17500, *et seq*.;

d. Whether Defendants' conduct is in violation of California Civil Code Sections 1709, 1710;

e. Whether Defendants' failure to implement effective security measures to protect Plaintiff's and the Class's Private Information negligent;

f. Whether Defendants breached express and implied warranties of security to the Class;

g. Whether Defendants represented to Plaintiff and the Class that they would protect Plaintiff's and the Class members' Private Information;

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

i. Whether Defendants breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

j. Whether Class members' PII was accessed, compromised, or stolen in the breach;

k. Whether Defendants' conduct caused or resulted in damages to Plaintiff and the Class;

l. Whether Defendants failed to notify the public of the breach in a timely and adequate manner;

m. Whether Defendants knew or should have known that its systems were vulnerable to a data breach;

n. Whether Defendants adequately addressed the vulnerabilities that allowed for the data breach; and

o. Whether, as a result of Defendants' conduct, Plaintiff and the Class are entitled to damages and relief.

73. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and the members of the Class were harmed by Defendants' uniform unlawful conduct.

74. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action and other complex litigation.

75. Plaintiff and the Class have suffered injury in fact as a result of Defendants' false, deceptive, and misleading representations.

76. Plaintiff would not have sent money through the Platform but for the reasonable belief that Defendants would safeguard his data and Private Information.

77. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

78. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

79. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendants' conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

80. Defendants have acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to

the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendants.

81. Absent a class action, Defendants will likely retain the benefits of its wrongdoing. Given the nature of individual Class members' claims, few, if any, could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Class members will continue to suffer losses and Defendants will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*

(Against Defendants MPSI and MGI on behalf of the California Subclass)

82. Plaintiff, individually and on behalf of the California Subclass, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

83. The California Unfair Competition Law ("UCL") prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

A. "Unfair" Prong

84. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

85. Defendants' conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendants would continue to store individual's data when it is unnecessary information for the handling of payments, such as when customers' identities have already been verified. Mishandling this data and a failure to archive and purge unnecessary data shows blatant disregard for customers' privacy and security.

86. Defendants did not need to collect the private data it did from its customers to allow use of the Platform. It did so to track and target its customers and monetize the use of the data to enhance its already exorbitant profits. Defendants utterly misused this data and Private Information.

87. Defendants' conduct as alleged herein causes injuries to consumers, who pay fees to send money on a Platform not consistent with their reasonable expectations of data security.

88. Defendants' conduct as alleged herein causes injuries to customers who entrusted Defendants with their Private Information and whose Private Information was leaked as a result of Defendants' unlawful conduct.

89. Defendants' failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

90. Consumers cannot avoid any of the injuries caused by Defendants' conduct as alleged herein.

91. The injuries caused by Defendants' conduct as alleged herein outweigh any benefits.

92. Defendants' conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

93. Defendants could have furthered its legitimate business interests in ways other than by unfair conduct.

94. Defendants' conduct threatens consumers by misleadingly advertising their Platform as "secure" and exposing consumers' Private Information to hackers. Defendants' conduct also threatens other companies, large and small, who play by the rules. Defendants' conduct stifles competition and has a negative impact on the marketplace and reduces consumer

choice.

95. All of the conduct alleged herein occurs and continues to occur in Defendants' business. Defendants' wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

96. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the California Subclass seek an order of this Court enjoining Defendants from continuing to engage, use, or employ its unfair business practices.

97. Plaintiff and the California Subclass have suffered injury-in-fact and have lost money or property as a result of Defendants' unfair conduct.

98. Plaintiff relied on and chose to use, and pay fees on, the Platform in part based on Defendants' representations regarding its security measures and trusted that Defendants would keep his Private Information safe and secure.

99. Plaintiff accordingly provided his Private Information to Defendants reasonably believing and expecting that his Private Information would be safe and secure.

100. Plaintiff paid unwarranted fees to use the Platform. Specifically, Plaintiff paid fees to use a Platform advertised as secure when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach.

101. Plaintiff and the California Subclass would not have utilized the Platform, or would not have given Defendants their Private Information, had they known that their Private Information was vulnerable to a data breach.

102. Plaintiff and the members of the California Subclass seek an order mandating that Defendants implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiff and the members of the California Subclass seek and request an order awarding Plaintiff and the California Subclass restitution of the money wrongfully acquired by Defendants by means of Defendants' unfair and unlawful practices. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasions of privacy for Plaintiff and the Class.

103. Plaintiff and California Subclass have no adequate remedy at law. As discussed above, at this time, in the absence of completed discovery regarding class certification and merits, forcing an election of remedies at the initial pleadings stage is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

B. "Fraudulent" Prong

104. California Business and Professions Code Section 17200, *et seq.* considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

105. Defendants' representations that it adequately protects customers' Private Information are likely to deceive members of the public into believing that MoneyGram can be entrusted with their Private Information, and that Private Information gathered by MoneyGram is not in danger of being compromised.

106. Defendants' representations about its products and services, as alleged in the preceding paragraphs, are false, deceptive, misleading, and unreasonable and constitute fraudulent conduct.

107. Defendants knew or should have known of its fraudulent conduct.

108. As alleged in the preceding paragraphs, the material misrepresentations by Defendants detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

109. Defendants could have implemented robust security measures to prevent the data breach but failed to do so.

110. Defendants' wrongful conduct is part of a pattern or generalized course of conduct.

111. Pursuant to Business & Professions Code Section 17203, Plaintiff and the California Subclass seek an order of this Court enjoining Defendants from continuing to engage,

use, or employ their practice of false and deceptive representations about the strength or adequacy of its security systems. Likewise, Plaintiff and the California Subclass seek an order requiring Defendants to disclose such misrepresentations.

112. Plaintiff and the California Subclass have suffered injury in fact and have lost money as a result of Defendants' fraudulent conduct. Plaintiff paid unwarranted fees to use the Platform. Plaintiff would not have utilized the services, if he had known that the Platform's use would put his Private Information at risk.

113. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the California Subclass seek an order of this Court compelling Defendants to implement adequate safeguards to protect all present and future customers' Private Information retained by Defendants, thereby seeking public injunctive relief that will benefit not only Plaintiff and the California Subclass but also the members of the general public. This includes, but is not limited to: improving security systems and verifications protocols of its employees and staff; limiting the access of customers' PII to only employees who need to have access to such PII to effectuate the transactions; deleting data that no longer needs to be retained by Defendants, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

114. California Business and Professions Code Section 17200, *et seq.*, identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

115. Defendants' unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

116. Defendants' conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

117. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring

reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law. Defendants failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

118. Defendants knew or should have known of its unlawful conduct.

119. As alleged in the preceding paragraphs, the misrepresentations by Defendants detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

120. Defendants could have furthered its legitimate business interests in ways other than by its unlawful conduct.

121. All of the conduct alleged herein occurs and continues to occur in Defendants' business. Defendants' unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

122. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the California Subclass seeks an order of this Court enjoining Defendants from continuing to engage, use, or employ its unlawful business practices.

123. Plaintiff and the California Subclass have suffered injury-in-fact and have lost money or property as a result of Defendants' unfair conduct. Plaintiff paid unwarranted fees to use the Platform. Specifically, Plaintiff paid to use a Platform advertised as secure when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the California Subclass would not have utilized the Platform, or would not have given Defendants their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiff and the members of the California Subclass seek an order mandating that Defendants implement adequate security practices to protect customers' Private Information. Additionally, Plaintiff and the members of the California Subclass seek and request an order awarding Plaintiff and the California Subclass restitution of the money

wrongfully acquired by Defendants by means of Defendants' unfair and unlawful practices. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the class.

COUNT TWO

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT

CALIFORNIA CIVIL CODE SECTION 1750, *et seq.*

(Against Defendants MPSI and MGI on behalf of the California Subclass)

124. Plaintiff, individually and on behalf of the California Subclass, repeats and realleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

125. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

126. Defendants are "persons" as that term is defined in California Civil Code § 1761(c).

127. Plaintiff and the California Subclass are "consumers" as that term is defined in California Civil Code §1761(d).

128. Defendants' unlawful conduct described herein was intended to increase the consuming public's use and fee payments for the use of its Platforms, and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the Platform has characteristics and benefits which it does not have.

129. Defendants fraudulently deceived Plaintiff and the California Subclass by representing that its Platform has certain characteristics, benefits, and qualities which it does not have, namely data protection and security. In doing so, Defendants intentionally misrepresented and concealed material facts from Plaintiff and the California Subclass, specifically by advertising secure technology when Defendants in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff and the California Subclass and depriving them of their legal rights and money.

130. Defendants' claims about its Platform led and continues to lead consumers like Plaintiff to reasonably believe that MoneyGram entities have implemented adequate data security measures when Defendants in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access customers' Private Information.

131. Defendants knew or should have known that adequate security measures were not in place and that customers' Private Information was vulnerable to a data breach.

132. Plaintiff and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendants' false representations.

133. Plaintiff and the California Subclass would not have utilized the Platform or would have accepted significantly reduced fees use of the Platform, had they known that their Private Information was vulnerable to a data breach, or that Defendants would fail to honor legal reporting requirements and leave them in the dark once their data was compromised.

134. Defendants' actions as described herein were done with conscious disregard of Plaintiff's rights, and Defendants were wanton and malicious in its concealment of the same.

135. Plaintiff and the California Subclass have suffered injury in fact and have lost money as a result of Defendants' unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff and the California Subclass paid unwarranted fees to use a Platform advertised as secure, and consequentially entrusted Defendants with their Private Information, when Defendants in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the California Subclass would not have utilized the Platform or would not have provided Defendants with their Private Information, had they known that their Private Information was vulnerable to a data breach.

136. Defendants should be compelled to implement adequate security practices to protect its customers' Private Information. Additionally, Plaintiff and the members of the California Subclass lost money as a result of Defendants' unlawful practices.

137. At this time, Plaintiff seeks public injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but he anticipates the need to amend the complaint and seek restitution.

COUNT THREE

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

(Cal. Civ. Code Section 1798.150, *Et Seq*.)

(Against Defendants MPSI and MGI on behalf of the California Subclass)

138. Plaintiff, individually and on behalf of the California Subclass, repeats and realleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

139. MoneyGram operated for profit or financial benefit of its owners with annual gross revenues over $1.3 billion.[32] MoneyGram is therefore, a business under the CCPA because it collects consumers' personal information, with the gross revenues in excess of twenty-five million dollars, that sells, buys, and/or shares the personal information of at least 100,000 or more consumers (as discussed above – it shares the personal information of 150 or more millions of consumers), and derives 50% or more of its annual revenues from selling or sharing consumers' personal information. MoneyGram also holds itself as the business under the CCPA, and provides various disclosures regarding its collection and use of personal information within its privacy notice.[33]

140. MoneyGram collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

141. Plaintiff is a "consumer" under Cal. Civ. Code § 1798.140(i) because he is a California resident, whose unredacted sensitive and personal information has been disclosed by MoneyGram as a result of unauthorized access, exfiltration, theft, and MoneyGram's failure to maintain reasonable security procedures appropriate to the nature of the information.

142. Specifically, MoneyGram violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the California Subclass Members' nonencrypted PII from unauthorized access and

[32] *Supra,* Note 1, at F-7 ("Consolidated Statements of Operations")
[33] https://www.moneygram.com/intl/privacy-center/global-privacy-notice (Local Supplements, D. CCPA and VCDPA)

exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

143. MoneyGram has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' PII. As detailed herein, MoneyGram failed to do so.

144. As a direct and proximate result of Defendants' acts, Plaintiff's and California Subclass Members' Private Information, including, names, contact information dates of birth, Social Security numbers, government-issued identification documents, bank account numbers, and transaction information., was subjected to unauthorized access and exfiltration, theft, or disclosure.

145. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure MoneyGram hereinafter adequately safeguards customers' Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because MoneyGram continues to hold customers' Private Information, including Plaintiff's and California Subclass Members' Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected, and MoneyGram has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by the Data Breaches.

146. As described herein, an actual controversy has arisen and now exists as to whether MoneyGram implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information under the CCPA.

147. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by MoneyGram and third parties with similar inadequate security measures.

148. Plaintiff and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

COUNT FOUR

DECEIT BY CONCEALMENT

(Cal. Civ. Code Sections 1709, 1710)

(Against Defendants MPSI and MGI on behalf of the California Subclass)

149. Plaintiff, individually, and on behalf of the California Subclass, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

150. MoneyGram knew or should have known that its security systems were inadequate to protect the Private Information of its customers. Specifically, MoneyGram had an obligation to disclose to its customers that its security systems were not adequate to safeguard their Private Information. MoneyGram did not do so. Rather, MoneyGram deceived Plaintiff and the California Subclass by concealing the vulnerabilities in its security system.

151. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendants' conduct as described herein therefore constitutes deceit of Plaintiff and the California Subclass.

152. California Civil Code §1709 mandates that in willfully deceiving Plaintiff and the California Subclass with intent to induce or alter their position to their injury or risk, MoneyGram is liable for any damage which Plaintiff and the California Subclass thereby suffer.

153. As described above, Plaintiff and the California Subclass have suffered significant harm as a direct and proximate result of Defendants' deceit and other unlawful conduct. Specifically, Plaintiff and the Class have been subject to numerous attacks, including various phishing scams. MoneyGram is liable for these damages.

COUNT FIVE

NEGLIGENCE

(Against Defendants MPSI and MGI on Behalf of the Nationwide Class, or Alternatively, on Behalf of the California Subclass)

154. Plaintiff, on behalf of the Nationwide Class, or alternatively, on behalf of the California Subclass, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

155. MoneyGram owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that customers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

156. This duty arises because it is foreseeable that the exposure of Private Information to unauthorized persons, especially to perpetrators of cyberattacks with nefarious intentions, will result in harm to the affected individuals, including, but not limited to: the invasion of their private data, the sale of their Private Information to facilitate identity theft, exposure to scams or phishing frauds, loss of time, economic damages as affected individuals scramble to protect their identities, and/or the countless ways these individuals' peace of mind is destroyed knowing their information is no longer secured.

157. Defendants' duties to use reasonable care also arose from several sources, including those described below. As referenced above, MoneyGram had a common law duty to prevent foreseeable harm to others, including Plaintiff and members of the Class, who were the foreseeable and probable victims of any inadequate security practices.

158. Defendants' duties also arose under Section 5(a) of the Federal Trade Commission Act ("**FTC Act**") (15 USC § 45) prohibits "unfair or deceptive acts or practices in or affecting

commerce." Defendants' failure to protect Plaintiff's and the Class members' Private Information constitutes an unfair or deceptive act or practice ("**UDAP**") because it (a) "causes or is likely to cause substantial injury to consumers;" (b) "cannot be reasonably avoided by consumers"; and (c) "is not outweighed by countervailing benefits to consumers or competition." As interpreted and enforced by the FTC, this includes the failure to use reasonable measures to protect customers' Private Information.

159. Defendants' duties arose in each state's data breach notification laws, which required MoneyGram to inform impacted customers when it learned their Private Information was accessed by a criminal. Those states relevant statutes are as follows: Alabama—Ala. Code § 8-38-10; Alaska—Alaska Stat. § 45.48.010 et seq; Arizona—Ariz. Rev. Stat. §§ 18-545; Arkansas—Ark. Code Ann. § 4-110-104; California—Cal. Civ. Code § 1798.82; Colorado—Colo. Rev. Stat. § 6-1-716; Connecticut—Conn. Gen. Stat § 36a-701b; Delaware—Del. Code Ann. tit. 6, § 12B-101 et seq.; District of Columbia—D.C. Code § 28- 3851 et seq.; Florida—Fla. Stat. § 501.171; Georgia—Ga. Code § 10-1-910, 10-1-912; Hawaii—Haw. Rev. Stat. § 487N-2; Idaho—Idaho Stat. § 28-51-104 to 28-51-107; Illinois—815 ILCS 530/10; Indiana—Ind. Code § 24-4.9-3-1; Iowa—Iowa Code § 715C.2; Kansas—Kan. Stat. Ann. § 50-7a01 et seq.; Kentucky—Ky. Rev. Stat. Ann. § 365.732; Louisiana—La. Rev. Stat. § 51:3071 et seq.; Maine—Me. Rev. Stat. tit. 10, § 1347 et seq.; Maryland—Md. Code Ann., Com. Law § 14-3504; Massachusetts—Mass. Gen. Laws ch. 93H § 3; Michigan—Mich. Comp. Laws § 445.63; Minnesota—Minn. Stat. § 325E.61; Mississippi—Miss. Code Ann. § 75-24-29; Missouri—Mo. Rev. Stat. § 407.1500; Montana—Mont. Code Ann. § 30-14-1704; Nebraska—Neb. Rev. Stat. §§ 87-802, 87-803; Nevada—Nev. Rev. Stat. § 603A.220; New Hampshire—N.H. Rev. Stat. Ann. § 359-C:20; New Jersey—N.J. Stat. § 56:8-163; New Mexico—N.M. Stat. Ann. § 57-12C-1 et seq.; New York—GBL § 899-aa and N.Y. State Tech. Law § 208; North Carolina—N.C. Gen. Stat § 75-65; North Dakota—N.D. Cent. Code § 51-30-01 et seq.; Ohio—Ohio Rev. Code § 1349.19; Oklahoma—Okla. Stat. § 74-3113.1; Oregon—Or. Rev. Stat. § 646A.604; Pennsylvania—73 Pa. Stat. § 2303; Rhode Island—R.I. Gen. Laws § 11-49.2-1 et seq.; South Carolina—S.C. Code Ann. § 39-1-90; South Dakota—

S.D. Codified Laws § 22-40-1; Tennessee—Tenn. Code Ann. § 47-18-2107; Texas—Tex. Bus. & Com. Code § 521.053; Utah—Utah Code § 13-44-201; Vermont—Vt. Stat. Ann. tit. 9, § 2430 et seq.; Virginia—Va. Code Ann. § 18.2-186.6; Washington—Wash. Rev. Code § 19.255.010; West Virginia—W. Va. Code § 46A-2A-101 et seq.; Wisconsin—Wis. Stat. § 134.98; Wyoming—Wyo. Stat. § 40-12-501 et seq.

160. MoneyGram knew or should have known that Plaintiff's and the Class members' Private Information is information that is frequently sought after by hackers.

161. MoneyGram knew or should have known that Plaintiff and the Class members would suffer harm if their Private Information was leaked.

162. MoneyGram knew or should have known that its security systems were not adequate to protect Plaintiff's and the Class Members' Private Information from a data breach, especially in light of the nature and sensitivity of the Private Information it collects and purports to safeguard.

163. MoneyGram knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiff, and the Class could have taken more swift and effective action to change or otherwise protect their Private Information. MoneyGram failed to provide timely notice upon discovery of the data breach. The general public was informed of the Data Breach on October 9, 2024. However, MoneyGram has yet to notify all of the Class Members about the data breach, and thus, is continuing to impose harm on all individuals by failing to disclose who is affected by the data breach. MoneyGram had learned of the data breach on September 27, 2024.

164. Defendants' conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Class members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information.

165. MoneyGram and the Class entered into a special relationship when the Class members entrusted MoneyGram to protect their Private Information. Plaintiff and the Class paid

fees to utilize Defendants' Platform, and in doing so provided MoneyGram with their Private Information, based upon Defendants' representations that it would implement adequate systems to secure their information. MoneyGram did not do so. MoneyGram knew or should have known that its security system was vulnerable to a data breach. MoneyGram breached its duty in this relationship to implement and maintain reasonable measures to protect the Private Information of the Class.

166. Plaintiff's and the Class members' Private Information would have remained private and secure had it not been for Defendants' wrongful and negligent breach of their duties. The leak of Plaintiff's and the Class members' Private Information, and all subsequent damages, was a direct and proximate result of Defendants' negligence.

167. Defendants' negligence was, at least, a substantial factor in causing the Plaintiff's and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class Members' other injuries because of the data breaches.

168. The damages suffered by Plaintiff and the Class members was the direct and reasonably foreseeable result of Defendants' negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiff and the Class Members' Private Information. MoneyGram knew or should have known that its security for safeguarding Plaintiff and the Class Members' Private Information was vulnerable to a data breach.

169. Defendants' negligence directly caused significant harm to Plaintiff and the Class.

COUNT SIX

INTENTIONAL MISREPRESENTATION

(Against Defendants MPSI and MGI on Behalf of the Nationwide Class, or Alternatively, on Behalf of the California Subclass)

170. Plaintiff, on behalf of the Nationwide Class, or alternatively, on behalf of the California Subclass, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

171. MoneyGram has represented, through online advertisements and its privacy policy,

that MoneyGram affords robust protection to its customers' Private Information.

172. MoneyGram makes representations that its security protections are multifaceted and effective, including the operation of "robust physical, technical, organizational, and administrative safeguards to protect [customers'] personal data from unauthorized access, loss or alteration."[34] and employing "preventive measures to restrict access to Personal Information to only those who have need to know"[35] MoneyGram in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

173. Defendants' misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' Private Information. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making their purchase decision.

174. At all relevant times when such misrepresentations were made, MoneyGram knew or should have known that the representations were misleading.

175. MoneyGram intended for Plaintiff and the Class to rely on the representations of its security systems, as evidenced by Defendants' intentional marketing of a safe and secure Platform.

176. Plaintiff and members of the Class reasonably and justifiably relied on Defendants' intentional misrepresentations when paying fees to utilize the Platform, and had they known the truth, they would not have utilized the Platform or would not have given MoneyGram their Private Information.

177. MoneyGram was negligent in its representations that it would provide the highest level of security for consumers.

178. As a direct and proximate result of Defendants' intentional misrepresentations, Plaintiff and members of the Class have suffered injury in fact.

---

[34] *Supra,* Note 4
[35] *Supra,* Note 8

COUNT SEVEN

BREACH OF EXPRESS WARRANTY

(Against Defendants MPSI and MGI on Behalf of the Nationwide Class, or Alternatively, on Behalf of the California Subclass)

179. Plaintiff, on behalf of the Nationwide Class, or alternatively, on behalf of the California Subclass, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

180. MoneyGram made an express warranty to Plaintiff and members of the Class that its security protections are multifaceted and effective. In order to utilize the Platform, Plaintiff and the Class were required to provide their Private Information which they reasonably believed, based on Defendants' expressed claims, would be kept private and secure.

181. Defendants' express warranty regarding its security standards it made to Plaintiff and the Class appears throughout its website and disclosures.[36] The promises of security associated with the products and services describe the products and services, specifically relates to the products/services being utilized and paid for, and therefore becomes the basis of the bargain.

182. Plaintiff and the Class paid fees for use of the Platform with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by MoneyGram on its website.

183. MoneyGram breached the express warranty made to Plaintiff and Class members by failing to provide adequate security to safeguard Plaintiff's and the Class's Private Information. As a result, Plaintiff and Class Members suffered injury and deserve to be compensated for the damages they suffered.

184. Plaintiff and Class Members paid fees for use of the Platform. However, Plaintiff and Class members did not obtain the full value of the advertised services. If Plaintiff and other Class members had known that their Private Information would be exposed, then they would not

[36] *See supra* notes 1-8.

have utilized the Platform, or would have paid substantially less in fees to utilize the Platform. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach.

COUNT EIGHT

UNJUST ENRICHMENT

(Against Defendants MPSI and MGI on Behalf of the Nationwide Class, or Alternatively, on Behalf of the California Subclass)

185. Plaintiff, on behalf of the Nationwide Class, or alternatively, on behalf of the California Subclass, herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

186. Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and Class Members.

187. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members was to be used to provide the necessary level of data security.

188. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased services from MoneyGram entities and in doing so provide Defendants with their most sensitive PII. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject to the transaction and have their PII protected with adequate data security measures.

189. Defendants knew that Plaintiff and Class Members conferred a benefit which MoneyGram accepted, and through which MoneyGram entities were unjustly enriched. Defendants profited from these transactions and used Plaintiff's and Class's PII for business purposes.

190. Defendants enriched themselves by saving the costs they reasonably should have spent on data security measures to secure Plaintiff's and Class's PII. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits, all at the expense of Plaintiff and the Class – by using ineffective security measures, failing to pay money for the much needed training of their

employees, failing to conduct the audits, and implement other security measures discussed above. Plaintiff and the Class suffered an injury as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and training.

191. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and the Class, because they failed to implement appropriate data management and security measures as mandated by the common law and statutory duties.

192. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant nor would they have used Defendant's services.

193. Plaintiff and the Class have no adequate remedy at law.

194. Defendants should be compelled to disgorge their profits and/or proceeds that they unjustly received as a result of having Plaintiff's and Class Members' PII, or alternatively, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment and relief on all cause of action as follows:

1. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;
2. That the Court enter an order declaring that Defendants' actions, as set forth in this Complaint, violate the laws set forth above;
3. An order:

a. Prohibiting MoneyGram from engaging in the wrongful acts stated herein (including MoneyGram's' failure to provide timely notice to all affected consumers);

b. Requiring MoneyGram to implement adequate security protocols and practices to protect consumers' Private Information consistent with industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring MoneyGram to protect all data collected through its account creation or verification requirements;

e. Requiring MoneyGram to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless MoneyGram can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. Requiring MoneyGram to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

g. Requiring MoneyGram to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on MoneyGram's systems on a periodic basis;

h. Requiring MoneyGram to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring MoneyGram to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak

of any additional information;

j. Requiring MoneyGram to conduct systematic scanning for data breach related issues;

k. Requiring MoneyGram to train and test its employees regarding social engineering protocols and appropriate responses to such attempts, including any necessary ongoing training, on a periodic basis, to ensure that its employees are well-versed in recognizing and capable of preventing, a social engineering attempt to access its data systems;

l. Requiring MoneyGram to train and test its employees regarding data breach protocols, verification procedures; archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII data; and

m. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted;

n. Requiring MoneyGram to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

o. Granting the public and the Class Members with public injunctive relief.

4. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

5. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against MoneyGram to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring MoneyGram to cooperate and financially support civil and/or criminal asset recovery efforts;

6. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);
7. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;
8. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and
9. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury for all claims.

DATED: November 25, 2024

Respectfully submitted,

By: */s/Yana Hart*

CLARKSON LAW FIRM, P.C.
Yana Hart, Esq.*
Mark I. Richards, Esq. (*PHV Forthcoming*)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
yhart@clarksonlawfirm.com
mrichards@clarksonlawfirm.com
**Admitted Pro Hac Vice*

BURNS CHAREST LLP
Darren Nicholson, Esq.
Chase Hilton, Esq.
Warren T. Burns, Esq.
900 Jackson Street, Suite 500
Dallas, TX 75202
Tel: (469) 914-7610
dnicholson@burnscharest.com
chilton@burnscharest.com
wburns@burnscharest.com

Counsel for Plaintiff and the Putative Classes