Dennis Stewart (#99152)
GUSTAFSON GLUEK PLLC
600 W. Broadway
Suite 3300
San Diego, CA 92101
Tel: (612) 333-8844
dstewart@gustafsongluek.com

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHELLE SALINAS and RAYMEL WASHINGTON, individually and on behalf of all others similarly situated, Plaintiffs, v. BLOCK, INC. and CASH APP INVESTING, LLC, Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Individually and on behalf of others similarly situated, Plaintiffs Michelle Salinas ("Salinas" or "Plaintiff Salinas") and Raymel Washington ("Washington" or "Plaintiff Washington") bring this action against Defendants Block, Inc. ("Block") and Cash App Investing, LLC, ("Cash App Investing") (collectively, the "Defendants"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys. Plaintiffs believe that substantial additional evidentiary support for the allegations set forth herein exists and will be revealed after a reasonable opportunity for discovery.

INTRODUCTION

1. This is a class action for damages against Defendants for their failure to exercise reasonable care in securing and safeguarding consumer information in connection with a massive December 2021 data breach (the "Data Breach") that resulted in the unauthorized public release of the personally identifiable information of 8.2 million current and former Cash App Investing customers, including Plaintiffs' and proposed "Class" (defined below) members' full names and brokerage account numbers (which are the personal identification numbers associated with Cash App Investing customers' stock activity on the Cash App Investing platform), the value and holdings of brokerage portfolios, and trading activity (collectively, the "PII" or "Private Information").[1]

2. According to Block's disclosure of the Data Breach, a former employee who had access to the Private Information belonging to Cash App Investing users during his tenure downloaded the data without Defendants' authorization.[2]

3. Cash App Investing is a stock trading platform by Block (formerly Square, Inc.). Accordingly, to the world of cybercriminals, Cash App Investing's customer list, which was in Defendants' possession and control at the time of the Data Breach, is highly valuable. By accessing Cash App Investing customers' PII entrusted to Defendants, hackers can gain access to Cash App Investing users' portfolios and account funds and use those funds to commit a wide range of fraudulent activities against the user, as was done here against Plaintiffs.

4. The security of Defendants' customers' Private Information is accordingly of the utmost importance. One instance of a former employee accessing, exfiltrating, and misusing and/or releasing for future misuse Plaintiffs' and Class members' Private Information to fellow

---

[1] *See* Defendant Block's regulatory filing with the United States Securities and Exchange Commission (the "SEC"), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001512673/000119312522095215/d343042d8k.htm (last accessed May 25, 2022).

[2] *See* https://www.cpomagazine.com/cyber-security/over-8-million-cash-app-users-potentially-exposed-in-a-data-breach-after-a-former-employee-downloaded-customer-information/ (last accessed May 25, 2022).

cybercriminals can lead to substantial financial losses. As Defendants acknowledge, "Future costs associated with this incident are difficult to predict."[3] These costs will not only impact Defendants' bottom line but, more importantly, the millions of Cash App Investing users whose Private Information is now in the hands of cybercriminals.

5. Because of the Data Breach, Plaintiffs' and Class members' Private Information has been compromised and their financial accounts are no longer secure, including their Cash App Investing portfolio.

6. Defendants understand the seriousness of the misuse of customers' PII, and purport to address these issues. For example, Defendants tout that they "take reasonable measures, including administrative, technical, and physical safeguards to protect [users'] information from loss, theft, and misuse, and unauthorized access, disclosures, alteration, and destruction."[4] However, some believe the Data Breach occurred due to "an orphaned account still active on a third-party SaaS application like a cloud storage solution," or due to "a lack of proper communication between the Human Resources and [] IT department on the status of terminated employees."[5]

7. While the exact reason(s) for the Data Breach remain unclear, there is no doubt that Defendants failed to adequately protect Plaintiffs' and Class members' Private Information and such negligent failures resulted in the injuries alleged herein.

8. Defendants led Plaintiffs and Class members to believe that their Private Information was safe and secure, and that protection of that Private Information was a fundamental component of the Cash App Investing platform.

---

[3] *See* https://www.sec.gov/ix?doc=/Archives/edgar/data/0001512673/000119312522095215/d343042d8k.htm (last accessed May 25, 2022).

[4] *Privacy Policy*, BLOCK, INC., https://cash.app/legal/us/en-us/privacy#security (last accessed May 25, 2022).

[5] *See* https://www.cpomagazine.com/cyber-security/over-8-million-cash-app-users-potentially-exposed-in-a-data-breach-after-a-former-employee-downloaded-customer-information/ (last accessed May 25, 2022).

9. Thus, on behalf of the Class of victims impacted by the Data Breach described herein, Plaintiffs seek, under state common law and consumer-protection statutes, to redress Defendants' misconduct.

PARTIES

Plaintiff Salinas

10. Plaintiff Salinas is a citizen of Texas and resides in Del Rio, Texas. Plaintiff Salinas became a Cash App Investing user in or around August of 2020. To invest through Cash App's investing feature, Plaintiff Salinas was required to provide her PII to Defendants' online service, including the types of PII mentioned above which was compromised in the Data Breach.

11. Plaintiff Salinas was led to believe that her Private Information was safe and secure, and that protection of her Private Information was a fundamental component of the Cash App Investing platform.

12. Following the Data Breach in December 2021 Plaintiff Salinas had multiple unauthorized charges on her Cash App account in December, 2021, and January 2022 totaling over $50. These charges were for Amazon purchases. Plaintiff Salinas has not been reimbursed by Defendants or Cash App for these unauthorized charges. As a result of the Data Breach, Plaintiff Salinas has spent over 100 hours researching the validity of the Data Breach, researching unauthorized charges and attempting to get reimbursement for them, searching through all of her financial accounts for unauthorized charges, resetting billing instructions that are tied to her Cash App account, researching credit monitoring, and dealing with false information that appeared on her Experian credit report following the Data Breach.

13. Plaintiff Salinas has suffered damages as described herein and below, including but not limited to, the fraudulent misuse of the funds in her Cash App account, and she remains at a significant risk of additional attacks now that her PII has been compromised and exfiltrated.

Plaintiff Washington

14. Plaintiff Washington is a citizen of Illinois and resides in Chicago, Illinois. Plaintiff Washington became a Cash App Investing user in or around September of 2019. To invest through Cash App's investing feature, Plaintiff Washington was required to provide his

PII to Defendants' online service, including the types of PII mentioned above and compromised in the Data Breach.

15. Plaintiff Washington was led to believe that his Private Information was safe and secure, and that protection of his Private Information was a fundamental component of the Cash App Investing platform.

16. On or around February 2022 through May of 2022 there were numerous unauthorized attempts to withdraw money from his account. These unauthorized transactions were declined because Plaintiff Washington did not have enough funds in his Cash App account to cover these fraudulent transactions. However, Defendants did not take any action because Plaintiff Washington had no funds taken from his account. On June 1, 2022, Plaintiff Washington was alerted to numerous unauthorized transactions in his Cash App account which totaled $394.85. Plaintiff Washington was unable to get that money back from Cash App. As a result of the Data Breach, Plaintiff Washington has spent at least 15 hours researching the validity of the Data Breach, researching unauthorized charges and attempting to get reimbursement for them, searching through all of his financial accounts for unauthorized charges, resetting billing instructions that are tied to his Cash App account, making a trip to the bank to get a new debit card that had to be cancelled as a result of the unauthorized charges, and researching credit monitoring.

17. Plaintiff Washington has suffered damages as described herein and below, including but not limited to, the fraudulent misuse of the funds in his Cash App account, and he remains at a significant risk of additional attacks now that his PII has been compromised and exfiltrated.

Defendant Block, Inc.

18. Defendant Block, Inc. is a Delaware corporation based in San Francisco, California.

19. Block, Inc. is the parent company of Defendant Cash App Investing, LLC and, by virtue of its relationship with Cash App Investing, had access to and possession of Plaintiffs' and Class members' PII, which it failed to secure by failing to implement adequate security measures

or screening procedures to ensure that its agents, support representatives, and other individuals to whom Defendants provided access to the PII would ensure its secure handling.

Defendant Cash App Investing, LLC

20. Defendant Cash App Investing is a limited liability brokerage firm and investment advisor firm with its main offices located at 400 SW 6th Avenue, 11th Floor, Portland, OR 97204.

21. Cash App Investing was formed in Delaware on February 22, 2019 and operates across the United States.

22. Cash App Investing is a subsidiary of Defendant Block, Inc. and, by virtue of its relationship with Block, had access to and possession of Plaintiffs' and Class members' PII, which it failed to secure by failing to implement adequate security measures or screening procedures to ensure that its current and/or former employees and other individuals to whom Defendants entrusted the Private Information would ensure its secure handling.

JURISDICTION AND VENUE

23. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class members, and the matter is a class action in which members of the class are citizens of a different state from that of a defendant.

24. This Court has personal jurisdiction since Defendant Block is headquartered in California and Defendants solicit customers and transact business in California. Plaintiffs are also informed and believe, and thereon allege, that acts and omissions giving rise to this action occurred in California.

25. Venue is also proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant Block resides within this district and acts and omissions giving rise to this action occurred within this District.

FACTUAL ALLEGATIONS

26. On or around December 10, 2021, Block determined that a former employee downloaded certain reports of its subsidiary, Cash App Investing, which contained U.S. customer Private Information. The Private Information was accessed without Defendants' permission.

27. In a recent regulatory filing with the SEC, Block disclosed the following as it relates to the Data Breach:

> "On April 4, 2022, Block, Inc. [] announced that it recently determined that a former employee downloaded certain reports of its subsidiary Cash App Investing LLC ("Cash App Investing") on December 10, 2021 that contained some U.S. customer information. While this employee had regular access to these reports as part of their past job responsibilities, in this instance these reports were accessed without permission after their employment ended.
>
> The information in the reports included full name and brokerage account number (this is the unique identification number associated with a customer's stock activity on Cash App Investing), and for some customers also included brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity for one trading day.
>
> The reports did not include usernames or passwords, Social Security numbers, date of birth, payment card information, addresses, bank account information, or any other personally identifiable information. They also did not include any security code, access code, or password used to access Cash App accounts. Other Cash App products and features (other than stock activity) and customers outside of the United States were not impacted.
>
> Upon discovery, the Company and its outside counsel launched an investigation with the help of a leading forensics firm. Cash App Investing is contacting approximately 8.2 million current and former customers to provide them with information about this incident and sharing resources with them to answer their questions.

> The Company is also notifying the applicable regulatory authorities and has notified law enforcement.[6]

28. Defendant Block offered no explanation for the four-month delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

29. Defendants' notice of the Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how the unauthorized former employee was able to access its networks, whether the Private Information accessed was encrypted or otherwise protected, or how it learned of the Data Breach. Even worse, Defendants failed to offer any credit or identity theft monitoring services for Plaintiffs and Class members.

30. Plaintiffs' and Class members' Private Information has been accessed, viewed, exfiltrated, and fraudulently misused to their detriment.

31. The Breach occurred because Defendants failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this release of information to former employees.

32. Defendants disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable administrative and data security measures to ensure that Plaintiffs' and Class members' PII was safeguarded from access by former employees. As a result, the Private Information of Plaintiffs and Class members were compromised through unauthorized access

---

[6] *See* https://www.sec.gov/ix?doc=/Archives/edgar/data/0001512673/000119312522095215/d343042d8k.htm (last accessed July 13, 2022).

resulting in damage to Plaintiffs and Class members. Plaintiffs and Class members have a continuing interest in ensuring that their Private Information is and remains safe.

Defendants' Privacy Promises

33. Defendants made, and continue to make, various promises to its customers, including Plaintiffs, that it will maintain the security and privacy of their Private Information.

34. In its Privacy Notice, Defendants state the following:[7]

> "We take reasonable measures, including administrative, technical, and physical safeguards, to protect your information from loss, theft, and misuse, and unauthorized access, disclosure, alteration, and destruction."[8]

35. By failing to do as they promised and protect Plaintiffs' and Class members' Private Information, and by allowing the Data Breach to occur, Defendants are in violation of their own Privacy Notice.

a. *Defendant Failed to Maintain Reasonable and Adequate Data Security Measures to Safeguard Customers' Private Information*

36. As a condition of engaging in financial-related services, Defendants require that customers entrust them with highly confidential Private Information. Defendants thus acquire, collect, and store a massive amount of their customers' protected Private Information, including financial information and other personally identifiable data By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class members' Private Information from unauthorized access.

37. Defendants had obligations created by industry standards, common law, and representations made to Plaintiffs and Class members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[7] *Privacy Notice*, https://cash.app/legal/us/en-us/privacy.

[8] *See* https://cash.app/legal/us/en-us/privacy#security.

38. Defendants failed to properly safeguard Plaintiffs' and Class members' Private Information, allowing at least one known unauthorized actor to access the Private Information.

39. Plaintiffs and Class members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants and any of their affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

40. Prior to and during the Data Breach, Defendants promised customers that their Private Information would be kept confidential.

41. Defendants' failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

42. In fact, Defendants have been on notice for years that Plaintiffs' and Class members' Private Information was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate administrative and data security measures to protect Plaintiffs' and Class members' Private Information from unauthorized access that Defendants should have anticipated and guarded against.

43. A 2021 study conducted by Verizon showed that internal mismanagement of data security represents nearly 44 percent of the data breaches in the financial sector.[9]

44. Private Information -related data breaches continued to rapidly increase into 2021 when Defendants' data were breached.[10]

[9] *Financial and Insurance Data Breaches*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.

[10] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

45. Almost half of data breaches globally are caused by internal errors relating to either human mismanagement of sensitive information or system errors.[11] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[12] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[13]

46. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[14]

47. To prevent and detect unauthorized access, including the access by the former employee(s) that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**

[11] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

[12] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[13] *Id.*

[14] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

48. These are basic, common-sense security measures that every business, not only those who handle sensitive financial information, should be taking. Defendants, with the highly sensitive personal and financial information in their possession and control, should be doing even more. By adequately taking these common-sense solutions, Defendants could have prevented this Data Breach from occurring.

49. Charged with handling sensitive Private Information, including financial information, Defendants knew, or should have known, the importance of safeguarding the Private Information that was entrusted to them and of the foreseeable consequences of a lapse

[15] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

in its data security. This includes the significant costs that would be imposed on Defendants' customers because of a breach. Defendants failed, however, to take adequate administrative cybersecurity measures to prevent the Data Breach from occurring.

50. The Private Information was maintained in a condition vulnerable to misuse. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiffs' and Class members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

The Monetary Value of Privacy Protections and Private Information

51. The fact that Plaintiffs' and Class members' Private Information was disclosed to bad actors that should not have had access to it—and has already been fraudulently misused—demonstrates the monetary value of the Private Information.

52. At all relevant times, Defendants understood Private Information it collects from its customers is highly sensitive and of significant property value to those who would use it for wrongful purposes.

53. Highly sensitive confidential information such as the Private Information accessed and misused here is a valuable and important commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes, including identify theft and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information including sensitive financial information on multiple underground Internet websites, commonly referred to as the dark web.

54. The Federal Trade Commission (the "FTC") has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

[16] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[17]

55. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[18] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

56. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2021 was, on average, $1,100.[19]

57. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Sensitive financial information can sell for as much as $1,000.[20] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's information, as is the case here.

58. The compromised Private Information in the Data Breach is of great value to thieves and can be used in a variety of ways. Information about, or related to, an individual for

---

[17] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

18 *Web's Hot New Commodity*, *supra* note 17.

19 *See* Megan Leonhardt, *Consumers lost $56 billion to identity fraud last year – here's what to look for* (March 23, 2021), https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html (last accessed July 5, 2022)

[20] *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Nov. 21, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/

which there is a possibility of logical association with other information is of great value to unauthorized actors that wish to use individuals' information for several nefarious purposes. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[21] For example, different Private Information elements from various sources may be linked in order to identify an individual, or access additional information about or relating to the individual.[22] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that was misused to perpetrate fraudulent purchases, applications for credit, and other identity theft in Plaintiffs' and Class members' names.

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

60. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to identity thieves as this information allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class members' Private Information to access accounts, including, but not limited to email accounts and other financial information, to engage in the fraudulent activity identified by Plaintiffs.

---

[21] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

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

61. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[23] This gives thieves ample time to make fraudulent charges under the victim's name.

62. Given these facts, any company that transacts business with customers and then causes and/or negligently permits the compromise of the privacy of customers' Private Information has thus deprived them of the full monetary value of their transaction with the company.

63. Plaintiffs and Class members have a property interest in their Private Information and were deprived of this interest when their Private Information was released to an unauthorized former employee because of Defendants' negligent administrative and data security practices.

b. ***Defendants Failed to Comply with FTC Guidelines***

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

65. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

[23] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[24] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

66. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[25] 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.

67. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

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

69. Defendants were, at all times, fully aware of their obligation to protect the Private Information of plan participants because of their position as a trusted financial and investment account administrator. Defendants were also aware of the significant repercussions that would result from their failure to do so.

[25] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[26] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter Start with Security].

c. *Damages to Plaintiffs and the Class*

70. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

71. The ramifications of Defendants' failure to keep its account holders' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches such as this are more likely to become victims of identity fraud.[27]

72. In addition to their obligations under state laws and regulations, Defendants owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to them, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

73. Defendants further owed and breached their duty to Plaintiffs and Class members to implement administrative processes and specifications as such relate to former employee access to customer Private Information that would have prevented the Data Breach from occurring.

74. As a direct result of Defendants' willful, reckless, and/or negligent conduct which resulted in the Data Breach, at least one known unauthorized party was able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse of Plaintiffs' and Class members' Private Information, as detailed above, and Plaintiffs and Class members remain at a heightened and increased risk of future identity theft and fraud.

75. The risks associated with identity theft are serious. Some identity theft victims spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or

[27] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

denied loans for education, housing or cars because of negative information on their credit reports.

76. Some of these risks associated with the loss of personal information have already materialized in the lives of Plaintiffs and Class members.

77. Plaintiffs and the Class have suffered or face a substantial risk of suffering out-of-pocket losses such as fraudulent charges on online accounts, credit card fraud, and similar identity theft.

78. Plaintiffs and Class members have, may have, and/or will incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

79. Plaintiffs and Class members did not receive the full benefit of the bargain made with Defendants and, instead, received services that were of a diminished value to that described in their agreements with Defendants. They were damaged in an amount at least equal to the difference in the value of the services *with* data security protection that they paid for and the services they actually received.

80. Plaintiffs and Class members would not have obtained services from Defendants had Defendants told them that it failed to properly train its employees, lacked administrative safety controls over the Private Information, and did not have proper data security practices to safeguard their Private Information from disclosure to unauthorized actors.

81. As a result of the Data Breach, Plaintiffs' and Class members' Private Information has also diminished in value.

82. The Private Information belonging to Plaintiffs and Class members is private in nature and was left inadequately protected by Defendants who did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person (especially not to a former employee), as required by Defendants' Privacy Notice, applicable law, and industry standards.

83. The Data Breach was a direct and proximate result of Defendants' failure to (a) properly safeguard and protect Plaintiffs' and Class members' Private Information from

unauthorized access, use, and disclosure, as required by their own Privacy Notice, various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such Private Information.

84. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligation to protect customer data.

85. Had Defendants remedied the deficiencies in their data security practices, procedures, and protocols and adopted adequate data security measures recommended by experts in the field, they would have prevented the intrusions into their systems by their former employee(s) and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

86. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family to mitigate the actual and potential impact of the Data Breach on their lives.

87. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[28]

88. Defendants' failure to adequately protect Plaintiffs' and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which consume time and expense while Defendants do nothing to assist those affected by the Data

[28] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

Breach. Instead, Defendants are putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft and mitigate such harms.

89. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing additional sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender, the individual provides sensitive information such as login credentials, account numbers, and the like.

90. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;

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

- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

- The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Private Information in its possession;

  Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

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

CLASS ACTION ALLEGATIONS

92. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

93. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3) and/or (c)(4).

94. Plaintiffs propose the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seek certification of the following Nationwide Class, California Subclass, Illinois Subclass and Texas Subclass (collectively defined herein as the "Class"):

Nationwide Class

All persons nationwide whose Private Information was compromised because of the Data Breach.

California Subclass

All persons residing in California whose Private Information was compromised because of the Data Breach.

Illinois Subclass

All persons residing in Illinois whose Private Information was compromised because of the Data Breach.

Texas Subclass

All persons residing in Texas whose Private Information was compromised because of the Data Breach.

Excluded from the Class are Defendants and Defendants' affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

95. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

96. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. According to Defendants, millions of individuals were affected by the Data Breach.

97. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

1. Whether Defendants' data security measures prior to and during the Data Breach complied with applicable data security laws and regulations;
2. Whether Defendants' data security measures prior to and during the Data Breach were consistent with industry standards;
3. Whether Defendants properly implemented their purported data security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;
4. Whether Defendants took reasonable measures to determine the extent of the Data Breach after it first learned of same;
5. Whether Defendants disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
6. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to

prevent unauthorized access to Plaintiffs' and the Class's Private Information;

7. Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

8. Whether Defendants were unjustly enriched by their actions; and

9. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

98. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of himself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both importance and number, to the numerous common questions that predominate in this action.

99. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

100. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Nationwide Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

101. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

102. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

103. Alternatively, to the extent the Court determines that Rule 23(b)(2) or Rule 23(b)(3) certification is not appropriate, the Court may certify a Rule 23(c)(4) issues class for determination of common material fact issues in the case, and/or liability.

COUNT I
NEGLIGENCE

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

104. Plaintiffs fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

105. Upon Defendants' accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as such.

106. Defendants owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

107. Defendants owed numerous duties to Plaintiffs and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b. to protect Private Information using reasonable and adequate administrative and data security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

108. Defendants also breached their duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

109. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate data security. Defendants knew or should have known about numerous well-publicized data breaches.

110. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

111. Defendants breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class members' Private Information.

112. Because Defendants knew that a breach of their systems would damage millions of their customers, including Plaintiffs and Class members, Defendants had a duty to adequately protect the Private Information.

113. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and their customers, which is recognized by laws and regulations including but not limited to common law. Defendants were in a position to ensure that their administrative and data security systems, practices, and protocols were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

114. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

115. Defendants are also bound by industry standards to protect confidential Private Information.

116. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information, which conduct included failing to: (1) secure Plaintiffs' and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent this type of data breach; and (5) failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

117. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate data security and failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen

and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendants' possession or control.

118. Defendants' conduct was negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

119. Neither Plaintiffs nor Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

120. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

121. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, strengthen data security systems and monitoring procedures, and immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF CONTRACT/BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

122. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

123. Plaintiffs and Class members entered into valid and enforceable express contracts with Defendants under which Plaintiffs and Class members agreed to provide their Private Information to Defendants, and Defendants agreed to provide financial services and to protect Plaintiffs' and Class members' Private Information.

124. In every contract entered into between Plaintiffs and Class members and Defendants, including those at issue here, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other

party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as Defendants were obligated to protect (and not interfere with) the privacy and protection of Plaintiffs' and Class members' Private Information.

125. To the extent Defendants' obligation to protect Plaintiffs' and Class members' Private Information was not explicit in those express contracts, the contracts also included implied terms requiring Defendants to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' Private Information, including in accordance with trade regulations; federal, state and local laws; and industry standards. No customer would have entered into these contracts with Defendants without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' express contracts.

126. A meeting of the minds occurred, as Plaintiffs and Class members agreed, among other things, to provide their Private Information in exchange for Defendants' agreement to protect the confidentiality of that Private Information.

127. The protection of Plaintiffs' and Class members' Private Information was a material aspect of Plaintiffs' and Class members' contracts with Defendants.

128. Defendants' promises and representations described above relating to industry practices and Defendants' purported concern about their clients' privacy rights became terms of the contracts between Defendants and their clients, including Plaintiffs and Class members. Defendants breached these promises by failing to comply with reasonable industry practices.

129. Plaintiffs and Class members read, reviewed, and/or relied on statements made by or provided by Defendants and/or otherwise understood that Defendants would protect their customers' Private Information if that information were provided to Defendants.

130. Plaintiffs and Class members fully performed their obligations under their contracts with Defendants; however, Defendants did not.

131. As a result of Defendants' breach of these terms, Plaintiffs and Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with Defendants; losing the difference in the value of

the services *with* adequate data security that Defendants promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports. Additionally, Plaintiff sand Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

132. Plaintiffs and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

133. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

134. Plaintiffs bring this claim alternatively to his claim for breach of contract.

135. Through their course of conduct, Defendants, Plaintiffs, and Class members entered into implied contracts for the provision of financial services, as well as implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

136. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendants when he first entered into financial services agreements with Defendants.

137. The valid and enforceable implied contracts to provide financial services that Plaintiffs and Class members entered into with Defendants include Defendants' promise to protect nonpublic Private Information given to them (or which Defendants created on its own from disclosure).

138. When Plaintiffs and Class members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

139. Defendants solicited and invited Plaintiffs and Class members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class members accepted Defendants' offer and provided their Private Information to Defendants.

140. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, and were consistent with industry standards.

141. Class members, including Plaintiff, who paid money to Defendants reasonably believed and expected that Defendant would use part of those funds to obtain and implement adequate data security measures. Defendants failed to do so.

142. Under implied contracts, Defendants and/or their affiliated providers promised and were obligated to: (a) provide financial services to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiffs and members of the Class agreed to pay money for these services, and to turn over their Private Information to Defendants.

143. Both the provision of financial services and the protection of Plaintiffs' and Class members' Private Information were material aspects of these implied contracts.

144. The implied contracts for the provision of financial services and maintenance of the privacy of Plaintiffs' and Class members' Private Information are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' Privacy Notice.

145. Defendants' express representations, including, but not limited to, the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and protect the privacy of Plaintiffs' and Class members' Private Information.

146. Consumers of financial services value their privacy and the ability to keep their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendants in the absence of the implied promise by Defendants to monitor the Private Information and to ensure that they adopted reasonable administrative and data security measures.

147. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendants and/or their affiliated companies, and paid for the provided services in exchange for, amongst other things, both the provision of financial services and the protection of their Private Information.

148. Plaintiffs and Class members performed their obligations under the contract when they paid for Defendants' services and provided their Private Information to Defendants.

149. Defendants materially breached their contractual obligation to protect the nonpublic Private Information they gathered when the Private Information was compromised as a result of the Data Breach.

150. Defendants materially breached the terms of these implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendants did not maintain the privacy of Plaintiffs' and Class members' Private Information as evidenced by their disclosures of the Data Breach to the SEC. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class members' Private Information as set forth above.

151. The Data Breach was a reasonably foreseeable consequence of Defendants' data security failures in breach of these contracts.

152. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain, and instead received financial and other services that were of a diminished value to that described

in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the difference in the value of the investing accounts *with* data security protection that they paid for and the services they actually received.

153. Had Defendants disclosed that their administrative and data security measures were inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiffs, Class members, nor any reasonable person would have utilized services from Defendants and/or their affiliated entities.

154. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

155. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

156. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.,* strengthen their data security systems and monitoring procedures, and immediately provide adequate credit monitoring to all Class members.

COUNT IV
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

157. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

158. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiffs and Class members should have received from Defendants the goods and services that were the subject of the transaction and should

have been entitled to have Defendants protect their Private Information with adequate data security.

159. Defendants knew that Plaintiffs and Class members conferred a benefit on them and accepted or retained that benefit. Defendants profited from Plaintiffs' purchases and used Plaintiff's and Class member's Private Information for business purposes.

160. Defendants failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' Private Information provided.

161. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

162. If Plaintiffs and Class members knew that Defendants would not secure their Private Information using adequate security, they would not have used Defendants' services.

163. Plaintiffs and Class members have no adequate remedy at law.

164. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

165. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and the Class members overpaid for the use of Defendants' services.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

166. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

167. In providing their Private Information to Defendants in exchange for financial services, Plaintiffs and Class members justifiably placed a special confidence in Defendants to

act in good faith and with due regard to the interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

168. Defendants accepted the special confidence Plaintiffs and Class members placed in them.

169. In light of the special relationship between Defendants and Plaintiffs and Class members, whereby Defendants became guardians of Plaintiffs' and Class members' Private Information, Defendants became fiduciaries by their undertaking and guardianship of the Private Information, to act primarily for the benefit of their customers, including Plaintiffs and Class members for the safeguarding of Plaintiffs' and Class member's Private Information.

170. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their customers' relationship, in particular, to keep secure the Private Information of their customers.

171. Defendants breached their fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class member's Private Information.

172. Defendants breached their fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiff's and Class members' Private Information.

173. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent preventing, detecting, contesting, and recovering from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued

possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendants' services they received.

174. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL"),

Cal. Bus. Prof. Code § 17200, *et seq.*,

(On Behalf of Plaintiffs and the California Subclass)

175. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

176. Defendants violated California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. By representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class member's Personal and financial information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiffs' and Class's Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. By soliciting and collecting Private Information from Plaintiff and Class members without adequately protecting or storing Private Information; and

c. By violating the California Customer Records Act, as set forth in further detail below.

177. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45.

178. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to, overpayments Defendants received to maintain adequate security measures and did not, the loss of their legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described above.

179. Defendants knew or should have known that their administrative and data security measures were inadequate to safeguard Plaintiff's and Class members' Private Information and that the risk of a data breach or unauthorized access was highly likely. Defendants had resources to secure and/or prepare for protecting customers' Private Information in a data breach. Defendants' actions in engaging in the above-named unfair, unlawful and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

180. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendants may have acquired by means of their deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

COUNT VII

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CRA"),

Cal. Bus. Prof. Code § 1798.80, *et seq.*,

(On Behalf of Plaintiffs and the California Subclass)

181. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

182. At all relevant times, Defendants were a "business" under the terms of the CRA, operating in the State of California and owning or licensing computerized data that included the Private Information of Plaintiffs and the Class.

183. At all relevant times, Plaintiffs and the Class were "customers" under the terms of the CRA as natural persons who provided personal information to Defendants for the purpose of purchasing or leasing a product or obtaining a service from Defendants.

184. Section 1798.82 requires disclosure "shall be made in the most expedient time possible and without unreasonable delay…." By the acts described above, Defendants violated the CRA by allowing unauthorized access to customers' personal and financial information and then failing to inform them for months when the unauthorized use occurred, thereby failing in their duty to inform their customers of unauthorized access expeditiously and without unreasonable delay.

185. The Data Breach described herein is a "breach of the security system" under Section 1798.82.

186. As a direct consequence of the actions as identified above, Plaintiffs and the Class incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and/or cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed, that they would have not otherwise lost had Defendants immediately informed them of the unauthorized use.

187. Plaintiffs accordingly request the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures.

188. Plaintiffs further request the Court require Defendants to identify all of their impacted clients, to what degree their information was stolen, and to notify all members of the Class who have not yet been informed of the Data Breach by written email within 24 hours of discovery of a breach, possible breach, and by mail within 72 hours.

189. As a result of Defendants' violations, Plaintiffs and the Class are entitled to all actual and compensatory damages according to proof, to non-economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

COUNT VIII

VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT,

815 ILCS §§ 505, *et seq*.

(On Behalf of Plaintiff Salinas and the Illinois Subclass)

190. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

191. Defendants are a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

192. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

193. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

194. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and

the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Salinas and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff Salinas and Illinois Subclass members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Salinas's and Illinois Subclass members' Private Information;

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

195. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

196. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Illinois Subclass members, that their

Private Information was not exposed and misled Plaintiff and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

197. Defendants intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

198. The above unfair and deceptive practices and acts by Defendants offend public policy, and were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

199. Defendants acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights.

200. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

201. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT IX
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILCS §§ 510/2, *et seq*.

(On Behalf of Plaintiff Salinas and the Illinois Subclass)

202. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

203. Defendants are a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(5).

204. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

205. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass

members' Private Information, including duties imposed by the FTC Act, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Illinois Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a)).

206. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

207. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Illinois Subclass members, that their Private Information was not exposed and misled Plaintiff and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

208. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

209. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

210. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT X

VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES ACT-CONSUMER PROTECTION ACT,

Texas Bus. & Com. Code §§ 17.41, *et seq.*,

(On Behalf of Plaintiff Washington and the Texas Subclass)

211. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

212. Defendants are a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

213. Plaintiff and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

214. Defendants advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

215. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

d. Defendants' false, misleading, and deceptive acts and practices include:

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

j. Failing to timely and adequately notify the Plaintiff and Texas Subclass members of the Data Breach;

k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Private Information; and

m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

216. Defendants intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

217. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

218. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Texas Subclass members, that their Private Information was not exposed and misled Plaintiff and the Texas Subclass members into believing they did not need to take actions to secure their identities.

219. Had Defendants disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants were trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Texas Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the Texas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

220. Defendant had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Texas Subclass, repose a trust and confidence in Defendants. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Texas Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Texas Subclass that contradicted these representations.

221. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

222. Consumers, including Plaintiff and Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience, or capacity to secure the Private Information in Defendants' possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Defendants' systems in order to evaluate its security controls. Defendants took advantage of its special skill and access to Private Information to hide its

inability to protect the security and confidentiality of Plaintiff and Texas Subclass members' Private Information.

223. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Defendants' unconscionable business acts and practices, exposed Plaintiff and Texas Subclass members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

224. Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights.

225. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information. Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiff and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

226. Defendants' violations present a continuing risk to Plaintiff and Texas Subclass members as well as to the general public.

227. Plaintiff and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for

each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT XI
DECLARATORY/INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the California, Illinois and Texas Subclasses)

228. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

229. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

230. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Private Information, and whether Defendants are currently maintaining data security measures, including employee (and former employee) practices, procedures, and protocols, adequate to protect Plaintiffs and Class members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at an imminent and substantial risk that further compromises of their Private Information will occur in the future.

231. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' Private Information.

232. Defendants still possesses the Private Information of Plaintiffs and the Class.

233. To Plaintiffs' knowledge, Defendants have made little, if any, changes to its data storage or security practices relating to the security of the Private Information.

234. To Plaintiffs' knowledge, Defendants have not adequately remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

235. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial.

236. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs, Plaintiffs and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

237. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

238. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors and internal personnel to run automated data security monitoring;

b. auditing, testing, and training their security personnel and employees regarding any new or modified procedures;

c. purging, deleting, and destroying Private Information not necessary for their provisions of services in a reasonably secure manner;

d. conducting regular database scans and security checks; and

e. routinely and continually conducting internal employee training and education to inform internal security personnel and employees how to prevent or detect

a similar data breach when it occurs and what to do in response to such a breach.

DEMAND FOR JURY TRIAL

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

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Defendants, as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, especially as such methods and policies pertain to both current and former employees;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e. Ordering Defendants to pay for not less than three (3) years of credit monitoring services for Plaintiffs and the Class;

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

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

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and such other and further relief as this court may deem just and proper.

Date: August 23, 2022

Respectfully submitted,

/s/Dennis Stewart
Dennis Stewart (#99152)
GUSTAFSON GLUEK PLLC
600 W. Broadway
Suite 3300
San Diego, CA 92101
Tel: (612) 333-8844
dstewart@gustafsongluek.com

Daniel E. Gustafson*
David A. Goodwin*
Mary M. Nikolai*
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
mnikolai@gustafsongluek.com

Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com
Jason S. Rathod*
jrathod@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Gary S. Graifman*
Melissa R. Emert*
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road, Suite 200
Montvale, New Jersey 07645
T: 845-356-2570
F: 845-356-4335
ggraifman@kgglaw.com
memert@kgglaw.com

Scott. D Hirsch*
SCOTT HIRSCH LAW GROUP
6810 N. State Road 7
Coconut Creek, FL 33073
(561) 569-7062
scott@scotthirschlawgroup.com

Counsel for Plaintiff and the Putative Class

**Pro Hac Vice Application to be Submitted*

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Michelle Salinas, et al.

(b) County of Residence of First Listed Plaintiff Val Verde County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Dennis Stewart, Gustafson Gluek PLLC, 660 W. Broadway, Suite 3300, San Diego, CA 92101 (612) 333-8844

DEFENDANTS

Block, Inc. and Cash App Investing, LLC

County of Residence of First Listed Defendant San Francisco County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § § 2201, et seq., 28 U.S.C §1332(d)(2)

Brief description of cause:
Negligence, Breach of Contract, Breach of Fiduciary Duty, State Consumer Protection Statutes, and Declaratory Judgment.

VII. REQUESTED IN COMPLAINT:

✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 08/23/2022 **SIGNATURE OF ATTORNEY OF RECORD** s/Dennis Stewart

ClassAction.org
