Robert S. Green (State Bar No. 136183)
James Robert Noblin (State Bar No. 114442)
Emrah M. Sumer (State Bar No. 329181)
GREEN & NOBLIN, P.C.
2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

Attorneys for Plaintiff,
AMANDA GORDON

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AMANDA GORDON, individually and on behalf of all other similarly situated, Plaintiff, vs. BLOCK, INC. and CASH APP INVESTING, LLC, Defendants.	Case No.: 3:22-cv-6787 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Amanda Gordon ("Gordon" or "Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to her and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants Block, Inc. ("Block") and Cash App Investing, LLC ("Cash App", the "App", and collectively "Defendants"), and allege as follows:

I. NATURE OF THE ACTION

1. Cash App, owned by Block, is a mobile application that allows users to transfer money from one person to another, while using the Cash App mobile application on their smartphone. Cash App also provides investing services which allows users to purchase stock and Bitcoin through its platform.

2. Cash App is widely used by many Americans, with over 50 million downloads on the Google Play store. It is also number one in the Apple store for free finance apps.

3. Cash App acquires and maintains extremely sensitive Personal Identifying Information ("PII") for each of its users. The security of Defendants' customers' inherently valuable PII is exceedingly important. Defendants are responsible for designing, developing, and maintaining the App's security measures, safely securing each user's PII, and actively monitoring third party infiltration. Due to Defendants' negligent security features, protocol, systems, screening, and design, however, Defendants failed to properly secure and protect App users' PII. Defendants' negligence has resulted in the exploitation and release of Cash App users' PII.

4. Defendants have known and/or should have known that its security measures, protocols, screening procedures, and systems were deficient in terms of how it fails to protect users' PII. This negligence and lack of action and due care by Defendants can be seen in postings about problems with the app and recently culminated in a recent data breach of the app. Defendants failed to take reasonable steps to safeguard consumer information in connection with a December 2021 data breach (the "Data Breach") that resulted in the unauthorized public release of PII of 8.2 million current and former Cash App Investing customers, including Plaintiff's and Proposed "Class" (defined below) members' full names and brokerage account

numbers (which are the personal identification numbers associated with Cash App customers' stock activity on the Cash App investing platform), the value and holdings of brokerage portfolios, and trading activity.[1]

5. According to Block's late disclosure of the Data Breach, a former employee who was given access to Class Members' PII by Defendants is believed to have, without authority, downloaded Plaintiff's and other consumer's PII.

6. PII is a commodity, bought and sold just like oil and gas, farm products, and precious minerals. Like other commodities, there is a thriving "black market" for PII, with hackers, thieves, organized crime, and individual actors seeking to acquire people's names, addresses, birthdays, tax identification numbers, and medical records to trade and sell. Defendants have contributed to this black market through their negligence and failure to exercise reasonable care.

7. Because of Defendants' negligence, Plaintiff and Class Members' PII has been compromised and their financial accounts, as well as accounts unrelated to Cash App, are not secure.

8. Defendants claim to understand the seriousness of their negligence and claim to be taking steps to address this failure. Defendants also claim 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."[2]

9. Despite Defendants' claims, 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."[3]

---

[1] *See* Defendant Block's regulatory filing with the United States Securities and Exchange Commission (the "SEC"), https://sec.report/Document/0001193125-22-006206/ (last accessed August 26, 2022).

[2] *Privacy Policy*, Block, Inc., https://cash.app/legal/us/en-us/privacy#security (last accessed August 25, 2022).

[3] *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 August 25, 2022).

10. By and through Defendants' negligence, they have caused financial losses and negative consequences and their negligence will continue to harm Class Members' into the future. Most importantly to the millions of Cash App users whose PII is in the hands of unauthorized third parties, due to Defendants negligence Class Members have either experienced damages and harm or it is likely that they will due to the Defendants negligence.

11. Thus, on behalf of the Class, Plaintiff seeks, under state common law and consumer-protection statutes, to redress Defendants' negligence.

II. PARTIES

Plaintiff Amanda Gordon

12. Plaintiff Gordon is a citizen of Texas and resides in Arlington, Texas. Plaintiff became a Cash App Investing user in or around July 2021. To invest through Cash App's investing platform, Gordon was required to provide her PII to Defendants, including the types of PII mentioned above, which is believed to have been accessed in the Data Breach.

13. Plaintiff Gordon reasonably believed Defendants would keep her PII secure as it was their duty to do so.

14. Following Defendants' negligence which resulted in her PII being accessed and/or stolen during the 2021 Data Breach, Plaintiff received multiple notices from credit monitoring services and even the Internal Revenue Service that bad actors had made use, and/or attempted to use, her PII. As a result of the breach, Plaintiff has been forced to lock her credit, spend time researching and responding to fraudulent transactions, spend time in an attempt to obtain reimbursement for fraudulent transactions, change her information on her other accounts, reset billing instructions tied to her Cash App account, and deal with false entries on her credit report. In addition, the Data Breach impacted her credit score and has made it difficult, and at times impossible, to access credit and benefits she was able to access prior to the Data Breach.

15. Plaintiff Gordon has suffered damages as described herein and she remains at significant risk from the ongoing and future damages now that her PII has been released to the public.

Defendants Block and Cash App

16. Defendant Block, Inc. is a Delaware corporation headquartered in San Francisco, California. Block, Inc. was formerly known as Square, Inc.

17. Block is the parent company of Cash App Investing, LLC and had access to and possession of Plaintiff's and Class Members' PII, which it failed to secure or protect with adequate security measures or screening procedures to ensure that its employees, agents, representatives, and other individuals to whom Defendants gave access to the Class's PII would handle said PII in a safe and secure manner.

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

19. Cash App was formed in Delaware in February 2019 and operates throughout the United States.

20. Cash App is a wholly owned subsidiary of Block and had access to and possession of Plaintiff's and Class Members' PII, which it failed to secure or protect with adequate security measures or screening procedures to ensure that its employees, agents, representatives, and other individuals to whom Defendants gave access to the Class's PII would handle said PII in a safe and secure manner.

III. JURISDICTION

21. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

22. This Court has personal jurisdiction over Defendants because they are registered to conduct business in California and have sufficient minimum contacts with California.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants conduct much of its business in this District and Defendants have caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Cash App Collects and Stores PII for its Own Financial Gain

24. Established in 2013 by parent company Square, Inc. (now known as Block), Cash App was one of the first peer-to-peer payment apps in the financial technology industry. Peer-to-Peer payment services allow consumers to use their smartphones to transfer money to individuals and businesses. In recent years, Cash App has expanded its services beyond Peer-to-Peer payments; Cash App users can now also receive direct deposit payments, purchase cryptocurrency, and invest through the app's investment feature.

25. When users establish an account with Defendants to use Cash App, users must provide Defendants with their PII, which Defendants then electronically collect and store.

26. Plaintiff and Class Members signed up for Cash App accounts and provided the required PII, which Defendants collected, stored, and routed through its servers.

27. In its "Privacy Notice," Defendants state the following:

> 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.
>
> *Privacy Notice*, https://cash.app/legal/us/en-us/privacy.

28. In this Privacy Notice Defendants conveniently omit to disclose the known inadequacies in their security system and protocol and prior known instances of hacking.

Defendants Turned a Blind Eye to Gaping Holes in its Security Despite User Complaints

29. Defendants were aware of inadequacies in its Cash App security prior to the December 2021 Data Breach. Since as early as 2020 Defendants have been repeatedly put on notice that its security measures were not up to par, leaving users' PII at risk of theft. Rather than addressing the problems by upgrading its security procedure, screening, system, and protocol, Defendants chose to allow Class Members' PII to remain potentially exposed to bad

actors. Defendants' negligence and failure to heed myriad warnings about its deficient data security, even after multiple hacking instances has shown Defendants' active concealment of the security inadequacy.

30. In fact, Defendants knew that Cash App users have been subject to a variety of fraudulent transfers from their Cash App accounts. An article published in March 2021 states six users were harmed by Cash App's vulnerability to hackers. In each of these instances, hackers accessed and drained cash, stock, and bitcoin out of accounts linked to Cash App.[4] Between August 2020 and September 2020, California business owner, Britt Soderberg, stated hackers generated numerous false refunds in Cash App, resulting in a loss of approximately $21,000.00.[5] In another attack, a Cash App user by the name of Shania Jensen, alleged that one morning she woke up to find that nearly $3,000.00 was drained from her account. [6] In yet another example, an individual, who chose to remain anonymous, alleged approximately $1,850.00 was taken out of his Cash-App linked bank account after he received what appeared to be a message with Cash App's official domain, stating there had been a fraudulent attempt to log into his account.[7] The user followed a link connecting him to his account, and double-checked his security settings. Despite this, the hackers began a series of cash withdrawals; he received no notifications from Cash App regarding any transactions.[8] Each of the above users claim they attempted to notify Cash App.

31. However, Cash App has been continuously criticized by its customers for its lack of action and communication. Those facing fraud concerning their Cash App account often cite it being nearly impossible to talk to a representative of Cash App on the telephone. Instead, users are most often met with communication loops where bots instead of humans handle their claims.

---

[4] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[5] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[6] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[7] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[8] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).

32. With increasing frustration surrounding Cash App's vulnerability from its users, the app has seen a surge in complaints. From February 2020, until March 2021 the Better Business Bureau investigated 2,485 complaints concerning Cash App.[9] This is in stark comparison to the mere 928 complaints filed for Venmo, and 83 complaints for Zelle during the same timeframe.[10]

33. However, the proverbial writing on the wall appeared in Cash App's user reviews. In February 2021, user reviews mentioning the words "fraud" or "scam" increased by 335% since February 2020.[11] This evidence shows that Cash App has been on continuous notice of its security inadequacies but has chosen to turn a blind eye to the issue. Cash App was well aware of security issues within its platform prior to the December 2021 Data Breach.

34. Defendants omitted essential facts concerning the App's lack of security, namely the App's known vulnerability to outside hackers. Had Cash App disclosed its app was regularly successfully attacked by outside hackers, Plaintiff and the Class would not have provided their PII to Cash App to set-up an account. Instead, because Plaintiff and the class were unaware of the prior successful hacking incidents, they put their PII at risk and continued to use Cash App. Cash App has profited off this material omission to the detriment of Plaintiff and the Class.

Defendants' Inadequate Data Security Causes 2021 Data Breach

35. Despite Defendants' knowledge of prior cybersecurity issues, Block disclosed the following information regarding a Data Breach in 2021:

> 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.

[9] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[10] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).
[11] https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed September 6, 2022).

> 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.

36. This notice was issued four (4) months after the Data Breach had allegedly occurred, and Block offered no explanation as to why they had let bad actors have a four (4) month head start on Plaintiff and Class Members who needed to protect their PII. This caused unnecessary damages and harm to Plaintiff and the Class.

37. Defendants failed to provide timely notice and when notice was issued, it was woefully insufficient. Defendants' notice failed to provide basic details including how the former employee accessed the PII, why a former employee had access to Defendants' networks, whether the PII was encrypted or protected in any way to keep bad actors from using it, or how the Data Breach was discovered. Further, Defendants did not offer any credit or identity theft monitoring services for Plaintiff and the Class.

38. By intentionally failing to disclose the Data Breach in a timely manner, Defendant misled consumers into continuing to use Defendants' services, thus providing Defendants with a continuous stream of income.

39. Plaintiff's and the Class's PII has been viewed, accessed, exposed, and misused because of Defendants' negligence, causing damages through fraudulent charges, lost time, and harm to their credit.

40. The Data Breach happened because Defendants failed to take reasonable measures to protect the Class's PII that Defendants had collected, stored, and were responsible for protecting.

41. Defendants disregarded the rights of Plaintiff and the Class by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable administrative and data security measures to ensure that Plaintiff's and the Class's PII was safeguarded from access by former employees. As a result, the PII of Plaintiff and the Class was compromised through unauthorized access resulting in damage to Plaintiff and the Class. Plaintiff and the Class have a continuing interest in protecting their PII.

Defendants Have Failed to Implement Reasonable Security Measures

42. Defendants require that customers trust them with highly confidential PII prior to customers being able to use Defendants' services. Defendants acquire, maintain, and store huge amounts of its customers' PII including their financial information and other personal data. By obtaining, collecting, using, and gaining a benefit from Plaintiff's and the Class's PII, Defendants assumed legal and equitable duties and knew, or should have known, they were responsible for protecting Plaintiff's and the Class's PII from unauthorized access.

43. Defendants were legally obligated by industry standards, common law, consumer protection statutes, and its own statements to Plaintiff and the Class to keep PII confidential and to protect it from unauthorized access and use.

44. Defendants failed to properly safeguard Plaintiff's and the Class's PII, allowing it to be accessed in an unauthorized fashion and for criminal purposes.

45. Plaintiff and the Class provided Defendants with their PII with the reasonable expectation and understanding that Defendants and any of its affiliates would comply with its obligations to keep such information secure, confidential, private, and safe from unauthorized access.

46. Defendants' failures to provide adequate security is especially egregious because Defendants do business in a field that has always been a frequent target of criminals and scammers seeking access to prized financial PII.

47. In fact, Defendants have been on notice for years that Plaintiff's and the Class's PII is a target for criminals. Despite this knowledge, Defendants have failed to implement and maintain reasonable and appropriate administrative and data security measures to protect Plaintiff and the Class's PII from criminal access that Defendants anticipated (as evidenced by its Privacy Notice) and should have guarded against.

48. As noted above, it is no longer a secret that PII is valuable, fungible, and the pot of gold at the end of the rainbow for cyber criminals.

Defendants Failed to Comply with FTC Guidelines

49. Defendants are forbidden from engaging in "unfair or deceptive acts or practices in or affecting commerce" by the Federal Trade Commission Act ("FTC Act"). 15 U.S.C. § 45. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumer's sensitive personal information is an "unfair practice" in violation of the FTC Act.[12]

50. The FTC has promulgated numerous guides for businesses that highlights 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.[13]

51. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[14] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on

[12] See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
[13] *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*].
[14] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf.

computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

52. The FTC further recommends that companies not maintain PII longer than is needed to authorize a transaction, limit access to PII, require complex passwords on networks, and verify that third-party service providers have implemented reasonable security measures. *See Start with Security*.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Defendants were, at all times, fully aware of their obligation to protect the PII of its users, including Plaintiff and the Class Members, because of its position as a trusted financial investment account administrator. Defendants were also aware of the significant repercussions that would, and have, resulted from their failure to protect its customers' PII.

Plaintiff and the Class Suffered Damages

55. The ramifications of Defendants' failure to implement adequate security measures on their platform are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[15]

56. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

57. Defendants required Plaintiff and Class Members to provide their PII, including full names and Social Security numbers. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class Members in its possession was only used

[15] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed July 28, 2021).

to provide the agreed-upon compensation and other employment benefits from Defendants.

58. Plaintiff and Class Members, therefore, did not receive the benefit of the bargain with Defendants, because providing their PII to Defendants was in exchange for Defendants' implied agreement to secure it and keep it safe.

59. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by 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 Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

60. Had Defendants disclosed that its app had been subject to prior successful hacks, Plaintiff and the Class would not have used Defendants' app, thus their PII would never have been provided to Defendants. Defendants' failure to provide this information is a material omission, on which the Plaintiff relied on to their detriment.

61. Defendants had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect customers' PII, and despite its Privacy Notice.

62. Had Defendants remedied the deficiencies in its data security training and protocols and adopted security measures recommended by experts in the field, they would have prevented the intrusion leading to the theft of PII.

63. As a direct and proximate result of Defendants' wrongful omissions, negligence, actions and inactions, Plaintiff 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.

64. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% 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."[16]

65. As a direct result of the Defendants' failures to implement adequate security measures, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

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

c. 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;

d. The continued risk to their PII, 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 PII in its possession; and

e. 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.

66. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

67. Defendants do not appear to be taking any measures to assist Plaintiff and Class Members.

[16] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 28, 2021).

68. Defendants' failure to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendants sit by and do nothing to assist those affected by their negligence. Instead, Defendants are putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

69. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when PII is acquired and when it is used. Even identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[17] Although their PII was improperly exposed in or about December 2021, affected current and former employees were not notified of the Data Breach until a year later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendants' delay in detecting and notifying customers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

V. CLASS ALLEGATIONS

70. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

> **Nationwide Class:** All persons who are current or former customers of Defendants or any of Defendants' affiliates, parents, or subsidiaries, and who have had their PII compromised as a result of Defendants' negligent security practices, procedures, screening, and protocols.

In addition, Plaintiff brings this action on behalf of the following proposed Texas subclass defined as follows:

> **Texas Subclass:** All persons residing in the State of Texas who are current or former customers of Defendants or any of

[17] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited July 28, 2021).

Defendants' affiliates, parents, or subsidiaries, and who have had their PII compromised as a result of Defendants' negligent security practices, procedures, screening, and protocols.

71. Both the proposed Nationwide Class and the proposed Texas Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

72. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

73. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

74. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' inadequate data security measures has resulted in compromising Plaintiff and the other Class Members' PII;

c. Whether Defendants owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiff and Class Members' PII in violation Section 5 of the FTC Act;

g. Whether Defendants actions violate the California Consumer Legal Remedies Act.

h. Whether Defendants have engaged in fraud;

i. Whether Defendants concealed the platform's inadequate security;

j. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

k. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

75. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

76. **Typicality.** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to Defendants' negligent security practices and had their PII accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

77. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

78. **Superiority.** 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 matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase 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 single adjudication, economies of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

79. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

80. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff and Class Members' PII in Defendants' possession was adequately secured and protected.

81. Defendants owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former customers.

82. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants

knew or should have known of the inherent risks in collecting and storing the PII of its current and former customers and allowing access to this information by terminated employees, and the critical importance of adequately securing such information.

83. Plaintiff and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard it, Defendants would not store it longer than necessary, and that Defendants were capable of protecting against the harm suffered by Plaintiff and Class Members because of the Data Breach.

84. Defendants' willful failure to abide by these duties was wrongful, reckless and grossly negligent as a business practice.

85. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendants' misconduct included failing to implement the necessary systems, policies, employee training, and procedures necessary to prevent the Data Breach.

86. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendants knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

87. Defendants breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

88. Plaintiff's injuries and damages, as described below, are a reasonably certain consequence of Defendants' breach of its duties.

89. Because Defendants knew that a breach of its systems would damage thousands of current and former customers, Defendants had a duty to adequately protect its data systems and the PII contained therein.

90. Plaintiff and Class Members reasonably believed that Defendants would take adequate security precautions to protect their PII. Defendants also had independent duties under

state and federal laws that required Defendants to reasonably safeguard Plaintiff and Class Members' PII.

91. Through Defendants' acts and omissions, including Defendants' failure to provide adequate security and its failure to protect Plaintiff and Class Members' PII from being foreseeably accessed, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class Members during the time it was within Defendants' possession or control.

92. In engaging in the negligent acts and omissions as alleged herein, Defendants failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendants have failed to do as discussed herein.

93. Defendants' failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

94. As a direct and proximate cause of Defendants' actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiff and Class Members have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to

undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

95. Lastly, Defendants had a special relationship with Plaintiff and Class Members, by virtue of the Plaintiff and Class Members being current or former customers of Defendants. The following factors support the existence of special relationship between Plaintiff and Class Members:

a. The harm caused to the Plaintiff and the Class was foreseeable. Defendants collected and stored the PII of the Plaintiff and the Class. Defendants understood that injury would occur to Plaintiff and the Class if their PII was not adequately protected and that a data breach would damage its current and former customers.

b. Defendants' services were intended to affect Plaintiff and the Class. Defendants developed an App specifically intended for those who sought the ease and access of investing and transferring funds electronically. This type of platform is not appealing to all consumers, rather, it is appealing only to a small subset of consumers who are seeking the ease and access described above. That small subset of consumers consists of Plaintiff and the Class Members. Plaintiff and the Class Members were specifically targeted by Defendants. By virtue of Defendants' services, Defendants intended to affect Plaintiff and the Class through their actions by entering into contracts with this specific subset of consumers, which required consumers to provide their PII before registering for Defendants' services.

c. There is a strong degree of certainty as to the injury sustained by Plaintiff and Class Members. The Plaintiff and Class Members suffered the following injuries:

i. the loss of the opportunity to determine for themselves how their PII is used;

ii. the publication and/or theft of their PII;

iii. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time;

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

v. costs associated with placing freezes on credit reports and password protection;

vi. anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

vii. the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; and

viii. future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and

continuing consequences of compromised PII for the rest of their lives

d. The injuries sustained by Plaintiff and the Class were a direct result of Defendants' lack of adequate, reasonable, and industry-standard security measures;

e. Defendants' conduct warrants moral blame because Defendants promised and failed to secure Plaintiff's and Class Member's PII, as evidenced by the Data Breach occurring in 2021; and

f. Holding Defendants accountable will require Defendants and other companies to provide reasonable, adequate, and industry-standard security measures in the future and will ensure data security is taken seriously by other companies.

COUNT TWO

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT – CALIFORNIA (CLRA) CIVIL CODE § 1750 *et seq.*
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

96. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

97. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale of goods or services to consumers. Defendants provided services to Plaintiff and the members of the class within the meaning of Cal. Civ. Code § 1761(b), and Defendants' acts, omissions, and practices as described herein fall under the CLRA.

98. Under the CLRA, a "consumer" is defined as someone who purchases services for personal, family, or household purposes. *Id.* at § 1761(d). Plaintiff and Class Members are consumers under this definition.

99. Defendants' material omissions and practices were and are likely to deceive consumers. Defendants were obligated to disclose material facts concerning its data security and failed to do so, resulting in its actions violating the CLRA. Defendants had exclusive knowledge

of the following undisclosed material facts, namely, that its security measures were (1) inadequate and unsecure; (2) subject to numerous hacking incidents; and (3) did not meet FTC guidelines. Despite knowledge of the foregoing Defendants withheld this knowledge from Plaintiff and the other members of the class.

100. Defendants' exclusive knowledge of its inadequate security measures and non-compliance with FTC guidelines, coupled with its contemporaneous knowledge of repeated hacking incidents occurring among its users, evidences Defendants' duty to disclose additional material facts.

101. Defendants' omissions and practices alleged herein violated the following provisions of Cal. Civ. Code § 1770, which provides in relevant part

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have…
> (7) Representing that goods or services are of a particular standard, quality, or grade … if they are of another.
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

102. Defendants stored the PII of Plaintiff and the other members of the class in its databases. However, Defendants failed to disclose that their system had been subject to prior hacking and that its security system and protocols did not comply with FTC guidelines.

103. Defendants knew or should have known that it did not employ reasonable measures to keep the PII or financial information of Plaintiff and the Class Members secure, to prevent the loss or misuse of the information. On numerous occasions Cash App users made complaints to Cash App that they had experienced hacking.

104. Defendants' deceptive acts and business practices induced Plaintiff and the Class Members to use its app and to provide their PII. But for these deceptive acts and practices,

Plaintiff and the other Class Members would not have provided their PII to Defendants or utilized its services. If Defendants had disclosed the security inadequacies, Plaintiff and the Class would have been aware and acted differently, by not utilizing Defendants' services or by taking extra precautions when using Defendants' services. By failing to disclose the security inadequacies, Defendants misled consumers into continuing use of Defendants' services, thus providing Defendants with a stream of income.

105. Plaintiff and Class Members were harmed as a result of Defendants' violations of the CLRA because their PII was compromised, placing them at a greater risk of identity theft. Plaintiff and the Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and Class Members have or will also suffer consequential out of pocket losses for procuring credit services, identity theft monitoring, and other expenses relating to identity theft losses and preventative measures.

106. Pursuant to Cal. Civ. Code § 1782, Plaintiff has notified Defendants in writing of the alleged violations of Cal. Civ. Code § 1770 and has demanded the same be corrected.

107. Pursuant to CLRA, Plaintiff and the Class are entitled to receive actual monetary damages (not to be less than one thousand dollars in class action lawsuits), punitive damages, injunctive relief against Defendants' unfair and deceptive business practices or acts, and attorney's fees and costs. *Id.* at § 1780.

COUNT THREE

FRAUD BY OMISSION
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

108. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

109. Defendants concealed or knowingly failed to disclose a material fact. Defendants had exclusive knowledge of the inadequacy of its security measures and contemporaneous knowledge that their security system did not meet FTC guidelines, but actively concealed these facts from Plaintiff and the class. Defendants were also aware that many of their users were experiencing hacking incidents on its platform.

110. Defendants had a duty to disclose the inadequacies of its security system. As a financial investment account administrator, Defendants collect sensitive PII from thousands of customers. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. Defendants' exclusive knowledge of its inadequate security measures and non-compliance with FTC guidelines, coupled with its contemporaneous knowledge of repeated hacking incidents occurring among its users, evidences Defendants' duty to disclose additional material facts. Thus, because of the special relationship between Plaintiff, Class Members, and the Defendants, Defendants had a duty to disclose to Plaintiff and Class Members that its security system did not have the robust measures needed to adequately protect the PII it required Plaintiff and Class Members to provide.

111. In order to induce consumers to utilize its app and continue its stream of income, Defendants failed to disclose its less than adequate security measures that did not comply with FTC guidelines and were already subject to prior instances of hacking.

112. Plaintiff and the class relied on Defendant's inadequate disclosures by utilizing its platform. Had Plaintiff and the Class known that Defendants were maintaining a less than industry standard security system and was subject to multiple hacking incidents, they would have taken other precautions or not used Defendants' services.

113. As a result of the foregoing, Plaintiff and the Class sustained damages when the 2021 Data Breach occurred, as alleged herein. Plaintiff and the Class Members suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit services, identity theft monitoring, and other expenses relating to identity theft losses and preventative measures.

COUNT FOUR

DECEIT BY CONCEALMENT – CAL. CIV. CODE §§ 1709 and 1710(3)
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

114. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

115. As alleged above, Defendants knew their data security measures were grossly inadequate, because its data security system did not comply with FTC guidelines, and it especially knew of the inadequacy after the Data Breach in 2021. Defendants also knew its platform was the subject of many hacking incidents among users. In response to these facts, Defendants chose to do nothing to protect Plaintiff and the class or warn them.

116. Defendants had an obligation to disclose to all Class Members that their accounts were an easy target for hackers as Defendants were not implementing a data security system in compliance with FTC guidelines and many users were already experiencing account hacking incidents.

117. Instead, Defendants did not make this disclosure. Defendants willfully deceived Plaintiff and the Class by concealing the true facts concerning their data security, which Defendants were obligated to and had a duty to disclose. Defendants' exclusive knowledge of its inadequate security measures and non-compliance with FTC guidelines, coupled with its contemporaneous knowledge of repeated hacking incidents occurring among its users, evidences Defendants' duty to disclose additional material facts.

118. Had Defendants disclosed the true facts about their dangerously poor data security, Plaintiff and the class would have either taken measures to protect themselves or not used Defendants' app at all. Plaintiff and the Class justifiably relied on Defendants to provide accurate and complete information about Defendants' security system, which it did not.

119. These actions are "deceit" under Cal. Civ. Code §1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

120. As a result of this deceit by Defendants, Defendants are liable under Cal. Civ. Code § 1709 for "any damage which [Plaintiff and the Class] thereby suffer []." Because of

Defendants' deceit, (1) the PII and financial information of Plaintiff and the Class was compromised, placing them at a greater risk of identity theft; (2) Plaintiff and the Class were subjected to identity theft; (3) Plaintiff and the Class's PII was accessed by a third party, without their consent (4) Plaintiff and the Class Members suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web; and (5) Plaintiff and Class Members have suffered consequential out of pocket losses for procuring credit services, identity theft monitoring, and other expenses relating to identity theft losses and preventative measures.

121. Defendants' deceit alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was "concealment of a material fact known to the defendant with the intention on the part of the defendant thereby depriving a person of property or legal rights or otherwise causing injury." As a result of the foregoing, Plaintiff and the Class are entitled to punitive damages against Defendants. *Id.* at § 3294(a).

COUNT FIVE

NEGLIGENT MISREPRESENTATION – CAL. CIV. CODE §§ 1709 and 1710(2)
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

122. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

123. There are four categories of deceit under California law, of those categories is negligent misrepresentation. *Id.* at § 1709-10. Negligent misrepresentation is defined as "the assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true." *Id.* at § 1710(2). Defendants negligently asserted the security of users' PII to their customers.

124. Defendants made the following assertion of material fact via its privacy policy – Defendants take reasonable precautions to protect users' information from theft, misuse, disclosure, and unauthorized access.

125. This assertion is false because if Defendants had taken reasonable precautions to protect consumers' PII, its security system would not have been the subject of a Data Breach in 2021, nor would it have been subject to prior hacking incidents as specified above.

126. Defendant made this assertion without any *reasonable* ground for believing it to be true. Defendants knew the system it had in place did not meet FTC guidelines and was subject to prior hacking incidents, therefore, they had no reasonable grounds to believe the security system was adequate or reasonable under the circumstances.

127. Defendant made this assertion with the intent that Plaintiff and the Class would rely on it. Defendants' misrepresentations made in its privacy policy, coupled with the failure to disclosure of prior instances of hacking and non-compliance with FTC guidelines, induced Plaintiff's and the Class's reliance. By making these negligent misrepresentations Defendant intended for Plaintiff and the Class to rely on them so that consumers would continue to use their services and its stream of income would not be affected. Thus, Defendant knew Plaintiff and Class Members would rely on this representation to their detriment and utilize its services.

128. Plaintiff and the Class were unaware of the falsity of Defendants' representation, otherwise they would not have utilized Defendants' services. Plaintiff had no reasonable way of knowing that Defendants were not utilizing adequate security measures or that many other users had been the subjects of hacking incidents. Plaintiff justifiably relied on this representation because the application was well-known and used by many other Americans.

129. As a result of Plaintiff's and the Class Members' reliance on the Defendants' negligent misrepresentations, Plaintiff and the Class Members sustained damages in the form of their PII being exploited, misused, and stolen. This is evidenced by the December 2021 Data Breach.

130. Defendants' misrepresentation was a substantial factor in causing the harm stated herein because had Defendants been honest about their inadequate security measures, Plaintiff and the Class would not have utilized Defendants' services or would have taken other precautions.

COUNT SIX

Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

131. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

132. Defendants offered services to its current or former customers, including Plaintiff and Class Members, in exchange for payment.

133. As a condition of its services, Defendants required Plaintiff and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, and other personal information. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class Members in its possession were only used to provide the agreed-upon benefits from Defendants.

134. These exchanges constituted an agreement between the parties: Plaintiff and Class Members would provide their PII in exchange for services and benefits provided by Defendants.

135. These agreements were made by Plaintiff or Class Members who were customers of Defendants.

136. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of services and benefits. Conversely, Defendants presumably would not have taken Plaintiff and Class Members' PII if it did not intend to provide Plaintiff and Class Members with services and benefits.

137. Defendants were therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

138. Plaintiff and Class Members accepted Defendants' offer and fully performed their obligations under the implied contract with Defendants by providing their PII, directly or indirectly, to Defendants, among other obligations.

139. Plaintiff and Class Members would not have provided and entrusted their PII to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII for other uses.

140. Defendants breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII.

141. Defendants' failure to implement adequate measures to protect the PII of Plaintiff and Class Members violated the purpose of the agreement between the parties.

142. Defendants were on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiff and Class Members' PII.

143. Instead of spending adequate financial resources to safeguard Plaintiff and Class Members' PII, which Plaintiff and Class Members were required to provide to Defendants, Defendants instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

144. As a proximate and direct result of Defendants' breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT EIGHT
Breach of Confidence
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

145. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

146. At all times during Plaintiff and Class Members' interactions with Defendants as its customers, Defendants were fully aware of the confidential and sensitive nature of Plaintiff and Class Members' PII that Plaintiff and Class Members provided to Defendants.

147. Plaintiff and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiff and Class Members' PII can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain certain PII without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of PII is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new PII in certain circumstances.

148. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff and Class Members' PII would

be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

149. Plaintiff and Class Members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

150. Defendants voluntarily received in confidence Plaintiff and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

151. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiff's and Class Members' PII, Plaintiff and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff and Class Members' confidence, and without their express permission.'

152. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

153. But for Defendants' disclosure of Plaintiff and Class Members' PII through its wrongful acts, in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff and Class Members' PII, as well as the resulting damages.

154. This disclosure of Plaintiff and Class Members' PII constituted a violation of Plaintiff and Class Members' understanding that Defendants would safeguard and protect the confidential and novel PII that Plaintiff and Class Members were required to disclose to Defendants.

155. The concrete injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff and Class Members' PII. Defendants knew its data security procedures for accepting and securing Plaintiff

and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiff and Class Members' PII in jeopardy.

156. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) 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 Plaintiff and Class Members.

COUNT NINE
Invasion of Privacy
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

157. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

158. Texas establishes the right to privacy in the Texas Constitution's Right to Privacy clause. *See* Tex. Const. Art. I, Section 9.

159. Texas further codified this right to privacy in the Texas Privacy Protection Act which went into effect on September 1, 2019. The Texas Privacy Protection Act requires businesses who collect PII only use and maintain PII that is relevant to accomplish the purpose for which the information was collected and that consumers must explicitly consent to the use and processing of that information. Tex. Bus. & Com. Code Ann. § 521.053 (West).

160. In addition, Defendants are required to create an "accountability program" and use due diligence in engaging a third party to processes PII. *Id.* If an individual has an account

with a business, and the individual closes that account, the business shall stop processing that individual's PII on the date the individual closes that account, delete the PII within 30 days (unless required by law), and notify any third parties that are processing that PII of the account closure. Defendants have failed to follow these protective measures. *Id.*

161. In addition, the Texas Privacy Protection act requires that businesses who suffer a data breach, like Defendants, must notify the affected individuals within sixty (60) days from the day the data breach was discovered. *Id.* Defendants did not provide notice for approximately four (4) months.

162. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

163. Defendants owed a duty to its employees, including Plaintiff and Class Members, to keep their PII private and confidential.

164. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

165. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiff and Class Members that was private and is entitled to remain private. Plaintiff and Class Members disclosed their PII to Defendants as part of their transaction with Defendants but did so privately with the intention and understanding the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendants' negligent actions and inactions, constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

167. Defendants invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligation to protect current and former customers' highly sensitive PII.

168. Defendants' motives leading to the Data Breach were financially based. In order to save on operating costs, Defendants decided against the implementation of adequate data security measures.

169. Defendants' intrusion upon Plaintiff and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

170. Acting with knowledge, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

171. As a proximate result of Defendants' acts and omissions, Plaintiff and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class Members to suffer concrete damages as described herein.

172. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendants can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

173. Plaintiff and Class Members have no adequate remedy at law for the injuries they have suffered and are at imminent risk of suffering in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT TEN
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

174. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

175. In light of its special relationship, Defendants became the guardian of Plaintiff and Class Members' PII. Defendants became a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of those customers, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff and Class Members' PII and to timely detect and notify them in the event of a data breach.

176. In order to provide Plaintiff and Class Members with services and to receive financial benefit for those services, Defendants required Plaintiff and Class Members provide their PII.

177. Defendants knowingly undertook the responsibility and duties related to the possession of Plaintiff and Class Members' PII for the benefit of Plaintiff and Class Members in order to provide Plaintiff and Class Members services and to make money.

178. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with them. Defendants breached its fiduciary duties owed to Plaintiff and Class Members by failing to properly encrypt and otherwise protect Plaintiff and Class Members' PII. Defendants further breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiff and Class Members of the Data Breach.

179. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) 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 researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

180. As a direct and proximate result of Defendants' breach of its fiduciary duty, Plaintiff 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 ELEVEN
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

181. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

182. As described above, when Plaintiff and the Class Members provided their PII to Defendants, they entered into implied contracts in which Defendants agreed to comply with its statutory and common law duties and industry standards to protect Plaintiff and Class Members' PII and to timely detect and notify them in the event of a data breach.

183. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their PII in exchange for services provided by Defendants.

184. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of services and benefits. Conversely, Defendants presumably would not have taken Plaintiff and Class Members' PII if it did not intend to provide Plaintiff and Class Members services and to receive financial benefits in return.

185. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon services and other benefits agreed upon between the Class Members and Defendants.

186. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendants, because they provided their PII in exchange for Defendants' implied agreement to keep it safe and secure.

187. While Defendants had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

188. Defendants breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff and Class Members' PII; storing the PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the customer relationship or transactions with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendants' data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

189. Plaintiff and Class Members did all or all the significant things that the contract required them to do.

190. Likewise, all conditions required for Defendants' performance were met.

191. Defendants' acts and omissions unfairly interfered with Plaintiff and Class Members' rights to receive the full benefit of their contracts.

192. Plaintiff and Class Members have been or will be harmed by Defendants' breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

193. Defendants are liable for its breach of these implied covenants, whether it is found to have breached any specific express contractual term.

194. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT TWELVE

Declaratory and Injunctive Relief
(On behalf of Plaintiff and Nationwide Class or, alternatively, the Texas Subclass)

195. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

196. This Count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. §2201.

197. As previously alleged, Plaintiff and Class Members entered an implied contract that required Defendants to provide adequate security for the PII it collected from Plaintiff and Class Members.

198. Defendants owe a duty of care to Plaintiff and Class Members requiring it to secure their PII.

199. Defendants still possess PII regarding Plaintiff and Class Members.

200. Since the Data Breach, Defendants have announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

201. Defendants have not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendants' insufficient data security is known to hackers, the PII in Defendants' possession is even more vulnerable to cyberattack.

202. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

203. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

204. Plaintiff, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants not transmit PII via unencrypted email;

f. Ordering that Defendants not store PII in email accounts;

g. Ordering that Defendants purge, delete, and destroy in a secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendants conduct regular computer system scanning and security checks;

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendants to meaningfully educate its current, former, and prospective customers about the threats they face because of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

COUNT THIRTEEN
Violations under Texas' Deceptive Trade Practices-Consumer Protection Act
Tex. Bus. & Com. Code § 17.41 et seq.
(On Behalf of the Texas Subclass)

205. Plaintiff incorporates the foregoing paragraphs as if fully set forth herein.

206. Defendants provide "services" under Tex. Bus. & Com. Code § 17.45(2) because they offer an App that allows consumers to purchase financial services.

207. Defendants are each a "person" under Tex. Bus. & Com. Code § 17.45(3) because they are each a corporation.

208. Plaintiff and the Texas Subclass Members are "consumers" under Tex. Bus. & Com. Code § 17.45(4) because they sought or acquired financial services through Defendants' App.

209. At all relevant times, Defendants have engaged in "trade" and "commerce" under Tex. Bus. & Com. Code § 17.45(6) by advertising, offering for sale, selling, and/or distributing their App in the United States, including Texas, directly or indirectly affecting Texas citizens through that trade and commerce.

210. The allegations set forth herein constitute false, misleading, or deceptive trade acts or practices in violation of Texas's Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Tex. Bus. & Com. Code § 17.41, *et seq.*

211. By failing to disclose prior hacking incidents and concealing the defective nature of the App's security features from Plaintiff and prospective Texas Subclass Members, Defendant violated the Texas Deceptive Practices Act as it represented that the App had

characteristics and benefits it did not have, represented that the App was of a particular standard, quality, or grade when it was of another.

212. Defendants' unfair and deceptive acts or practices occurred repeatedly in Defendant's trade or business, were capable of deceiving a substantial portion of the Texas Subclass and imposed a serious financial safety risk on the public.

213. Defendant knew that the App suffered from repeated hacking incidents, and had inadequate security measures in place that did not comply with FTC guidelines, which made the App not suitable for its intended use.

214. Defendant was under a duty to Plaintiff and the Texas Subclass to disclose the prior hacking incidents and security vulnerabilities of the App because:

a. Defendant was in a superior position to know the true state of facts surrounding the inadequate security measures associated with the App and the prior hacking incidents;

b. Plaintiff and the Texas Class Members could not reasonably have been expected to learn or discover that the App had deficient security features and prior hacking incidents until after they began using Defendants' financial services in the App; and

c. Defendant knew that Plaintiff and the Texas Subclass Members could not reasonably have been expected to learn about or discover the App's security inadequacies or prior hacking instances.

215. The facts concealed or not disclosed by Defendant to Plaintiff and the Texas Subclass are material in that a reasonable person would have considered them to be important in deciding whether or not to use CashApp.

216. Plaintiff and the Texas Subclass relied on Defendants to disclose material information it knew, such as the inadequate security features of the App, and not to induce them into a transaction they would not have entered had Defendants disclosed this information.

217. By failing to disclose the inadequacies of the App's security and the prior hacking instances suffered by Cash App, Defendant knowingly and intentionally concealed material facts and breached its duty not to do so.

218. Moreover, Defendant's intentional concealment of and failure to disclose the security inadequacies and prior instances of hacking constitutes an "unconscionable action or course of action" under Tex. Bus. & Com. Code § 17.45(5) because, to the detriment of Plaintiff and the Texas Subclass, that conduct took advantage of their lack of knowledge, ability, and experience to a grossly unfair degree. That "unconscionable action or course of action" was a producing cause of the economic damages sustained by Plaintiff and the Texas Subclass.

219. The facts concealed or not disclosed by Defendant to Plaintiff and the other Texas Subclass Members are material because a reasonable consumer would have considered them to be important in deciding whether or not to utilize Defendants' financial services offered through their platform, CashApp.

220. Had Plaintiff and other Texas Subclass Members known that the App had inadequate security features and had been the target of prior hacking instances, they would not have utilized CashApp or would have taken other precautions to protect their PII.

221. Plaintiff and the other Texas Subclass Members are reasonable consumers who do not expect that their PII will be subject to improper use while using Defendants' App. That is the reasonable and objective consumer expectation for using a financial App.

222. As a result of Defendant's misconduct, Plaintiff and the other Class Members have been harmed and have suffered actual and economic damages. Plaintiff and the other Class Members PII was compromised, placing them at a greater risk of identity theft. Plaintiff and the Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and Class Members have or will also suffer consequential out of pocket losses for procuring credit services, identity theft monitoring, and other expenses relating to identity theft losses and preventative measures.

223. Plaintiff Sanchez has provided adequate notice to Defendant. [18]

224. Plaintiff and the Texas Subclass should be awarded three times the amount of their economic damages because Defendant intentionally concealed and failed to disclose the known security inadequacies in CashApp and the prior hacking incidents.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of herself and all others similarly situated, respectfully request the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendants engaged in negligent and unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

[18] Plaintiff has mailed a letter to Defendants, pursuant to V.T.C.A., Bus. & C. Code § 17.505, giving written notice of the action prior to filing suit.

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members' PII;

v. prohibiting Defendants from maintaining Plaintiff and Class Members' PII on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities

with handling PII, as well as protecting the PII of Plaintiff and Class Members;

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

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with

compliance of the Court's final judgment;

xviii. requiring Defendants to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendants to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiff and Class Members damages;

f. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

I. JURY TRIAL DEMAND

Plaintiff, on behalf of herself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

DATED: November 2, 2022

GREEN & NOBLIN, P.C.

By: /s/ Robert S. Green
Robert S. Green

James Robert Noblin
Emrah M. Sumer
2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

William B. Federman*
Joshua D. Wells*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com
jdw@federmanlaw.com
**pro hac vice application forthcoming*

Attorneys for Plaintiff,
AMANDA GORDON

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

AMANDA GORDON, individually and on behalf of all other similarly situated

(b) County of Residence of First Listed Plaintiff Tarrant County , Texas
(EXCEPT IN U.S. PLAINTIFF CASES)

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

GREEN & NOBLIN, P.C., 2200 Larkspur Landing Circle, Suite 200, Larkspur, CA 94939
(415) 477-6700

DEFENDANTS

BLOCK, INC. and CASH APP INVESTING, LLC

County of Residence of First Listed Defendant
(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
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☒ 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. § 1332(d)

Brief description of cause:
Negligent misrepresentation in connection with data breach and loss of consumer data

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 11/02/2022 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Robert S. Green

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.