UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHELLE SALINAS, RAYMEL WASHINGTON, and AMANDA GORDON, individually and on behalf of all others similarly situated, Plaintiffs, v. BLOCK, INC. and CASH APP INVESTING, LLC, Defendants.	**Case No. 3:22-cv-04823** **CONSOLIDATED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiff Michelle Salinas ("Salinas"), Raymel Washington ("Washington") and Amanda Gordon ("Gordon") (collectively, "Plaintiffs), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and upon information and belief as to all other matters, and by and through their undersigned counsel, hereby bring 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.

2. Additionally, Cash App provides investing services which allows users to purchase stock and Bitcoin through its platform.

3. Cash App is widely used by many Americans, with over 50 million downloads on the Google Play store.

4. In conjunction with the services Cash App provides, Cash App acquires and maintains extremely sensitive Personal Identifying Information ("PII") for each of its users.

5. The security of Defendants' customers' inherently valuable PII is exceedingly important.

6. 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.

7. Unfortunately, due to Defendants' negligent security features, protocol, systems, screening, and design, Defendants suffered at least two data breaches in the last two years. Moreover numerous individuals have complained of unauthorized access to and transactions stemming from their Cash App accounts.

8. These instances make it apparent Defendants have utterly failed to properly secure and protect customer accounts and the users' PII accessible through the App, in multiple respects, which led to (among other things): (i) unauthorized access to the customer accounts; (ii) unintended transactions associated with customer Cash App accounts that were not appropriately resolved; (iii) the loss of the opportunity for customers to determine for themselves how their PII is used; and/or (iv) the publication and/or theft of their PII.

9. Multiple users have also complained about delays and other issues with Cash App's resolution process for addressing payment errors.

10. Defendants have known and/or should have known that their security measures, protocols, screening procedures, and systems were deficient in terms of how they fail to protect against unauthorized access to (and unauthorized transactions from) customer accounts and users'

PII stored therein. Defendants have also known and/or should have known that their procedures for resolving user complaints in response to such unauthorized access or unauthorized or unintended transactions were deficient. 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 recent data breaches of the app.

11. Defendants failed to take reasonable steps to safeguard consumer information in connection with a December 2021 data breach (the "First Data Breach") that resulted in the unauthorized public release of PII of 8.2 million current and former Cash App Investing customers, including Plaintiffs' and Proposed "Class" (defined below) members' full names and brokerage account numbers (which are the personal identification numbers associated with Cash App customers' stock activity on the Cash App investing platform), the value and holdings of brokerage portfolios, and trading activity.1

12. 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 Plaintiffs' and other consumer's PII.

13. Defendants' failure to take adequate security measures following the First Data Breach resulted in a second data breach in 2023 in which Cash App identified unauthorized access to customers' accounts, unauthorized transactions resulting from that access, and unauthorized access to customers' PII and account information2 (the "Second Data Breach", collectively with the First Data Breach, the "Data Breaches").

---

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 Aug. 26, 2022).

2 Including users' Cash App account number and routing number, Cash App Card number, expiration date, and CVV

14. 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.

15. Because of Defendants' negligence, Plaintiffs and Class Members' PII has been compromised and their financial accounts, as well as accounts unrelated to Cash App, are not secure, and were subject to unauthorized transactions. As a result, among other things, potential class members' accounts were accessed without authorization and/or used by unauthorized actors, class members had money taken from their accounts, stolen funds were not refunded or were only partially refunded, and data associated with Cash App accounts was used in various unauthorized ways. Moreover, Defendants failed to respond appropriately to reports of these issues.

16. 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."[3]

17. Despite Defendants' claims, some believe the First 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."[4]

---

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

4 *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 Aug. 25, 2022).

18. Ultimately, Defendants' claims of reasonable conduct are belied by the occurrence of not one but two data breaches and a flood of complaints from users that have had money stolen from their Cash App accounts and that have encountered problems in the error resolution process.

19. By and through Defendants' negligence, they have caused financial losses, most directly in the form of money being stolen out of users' vulnerable accounts by third parties, 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.

20. Thus, on behalf of the Class, Plaintiffs seek, under state common law and consumer-protection statutes, to redress Defendants' negligence.

II. PARTIES

Plaintiff Michelle Salinas

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

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

23. As a result of the First Data Breach, Plaintiff Salinas has spent over 100 hours researching the validity of the First Data Breach, researching unauthorized charges and attempting to get reimbursement for them, searching through all of her financial accounts for unauthorized

charges, resetting billing instructions that are tied to her Cash App account, researching credit monitoring, and dealing with false information that appeared on her Experian credit report following the First Data Breach.

24. In addition, as a result of Defendants' inadequate security measures, Plaintiff Salinas had multiple unauthorized charges on her Cash App account in December, 2021, and January 2022 totaling over $50. These charges were for Amazon purchases. Plaintiff Salinas has not been reimbursed by Defendants or Cash App for these unauthorized charges.

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

Plaintiff Raymel Washington

26. Plaintiff Washington is a citizen of Illinois and resides in Chicago, Illinois.

27. Plaintiff Washington became a Cash App Investing user in or around September of 2019 to invest through Cash App's investing feature. Plaintiff Washington was required to provide PII to Defendants' online service, including the types of PII mentioned above and compromised in the First Data Breach.

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

29. As a result of the First Data Breach, Plaintiff Washington has spent at least 15 hours researching the validity of the First Data Breach, researching unauthorized charges and attempting to get reimbursement for them, searching through all of his financial accounts for unauthorized charges, resetting billing instructions that are tied to his Cash App account, making a trip to the

bank to get a new debit card that had to be cancelled as a result of the unauthorized charges, and researching credit monitoring.

30. In addition, as a result of Defendants' inadequate security measures, on or around February 2022 through May of 2022 there were numerous unauthorized attempts to withdraw money from his account. These unauthorized transactions were declined because Plaintiff Washington did not have enough funds in his Cash App account to cover these fraudulent transactions. However, Defendants did not take any action because Plaintiff Washington had no funds taken from his account.

31. On June 1, 2022, Plaintiff Washington was alerted to numerous unauthorized transactions in his Cash App account which totaled $394.85. Plaintiff Washington reported these unauthorized transactions to Defendants, but he was unable to get that money back from Cash App.

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

Plaintiff Amanda Gordon

33. 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 First Data Breach.

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

35. Following Defendants' negligence which resulted in her PII being accessed and/or stolen during the First 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 First 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 First Data Breach.

36. 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

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

38. Block is the parent company of Cash App Investing, LLC and had access to and possession of Plaintiffs' 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.

39. 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.

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

41. Cash App is a wholly owned subsidiary of Block and had access to and possession of Plaintiffs' 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

42. 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.

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

44. 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

45. 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.

46. 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.

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

48. 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.

49. 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

50. Defendants were aware of inadequacies in its Cash App security prior to the First 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.

51. 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.[5] 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.[6] 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. [7] 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.[8] 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.[9] Each of the above users claim they attempted to notify Cash App.

52. However, Cash App has been continuously criticized by its customers for its lack of action and communication, and for deficiencies in its error resolution processes for determining whether electronic funds transfers alleged to be unauthorized must be reimbursed under relevant regulations. 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.

---

5 https://www.yahoo.com/lifestyle/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html (last accessed Sept. 6, 2022).
6 *Id.*
7 *Id.*
8 *Id.*
9 *Id.*

53. 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.10 This is in stark comparison to the mere 928 complaints filed for Venmo, and 83 complaints for Zelle during the same timeframe.11

54. 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 2020.12 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 First Data Breach.

55. 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, Plaintiffs and the Class would not have provided their PII to Cash App to set-up an account. Instead, because Plaintiffs 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 Plaintiffs and the Class.

Defendants' Inadequate Data Security Causes First Data Breach

56. Despite Defendants' knowledge of prior cybersecurity issues, Block disclosed the following information regarding a First 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

10 *Id.*
11 *Id.*
12 *Id.*

> their past job responsibilities, in this instance these reports were accessed without permission after their employment ended.
>
> The information in the reports included full name and brokerage account number (this is the unique identification number associated with a customer's stock activity on Cash App Investing), and for some customers also included brokerage portfolio value, brokerage portfolio holdings and/or stock trading activity for one trading day.
>
> The reports did not include usernames or passwords, Social Security numbers, date of birth, payment card information, addresses, bank account information, or any other personally identifiable information. They also did not include any security code, access code, or password used to access Cash App accounts. Other Cash App products and features (other than stock activity) and customers outside of the United States were not impacted.
>
> Upon discovery, the Company and its outside counsel launched an investigation with the help of a leading forensics firm. Cash App Investing is contacting approximately 8.2 million current and former customers to provide them with information about this incident and sharing resources with them to answer their questions. The Company is also notifying the applicable regulatory authorities and has notified law enforcement.

57. This notice was issued four (4) months after the First 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 Plaintiffs and Class Members who needed to protect their PII. This caused unnecessary damages and harm to Plaintiffs and the Class.

58. 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 First Data Breach was discovered. Further, Defendants did not offer any credit or identity theft monitoring services for Plaintiffs and the Class.

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

60. Plaintiffs' 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.

61. The First 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.

62. Defendants disregarded the rights of Plaintiffs 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 Plaintiffs' and the Class's PII was safeguarded from access by former employees. As a result, the PII of Plaintiffs and the Class was compromised through unauthorized access resulting in damage to Plaintiffs and the Class. Plaintiffs and the Class have a continuing interest in protecting their PII.

Defendants' Inadequate Data Security Causes a Second Data Breach in 2023

63. Incredulously, Defendants' knowledge of prior cybersecurity issues, as well as the First Data Breach, Defendants disclosed in June of 2023 the following information regarding a second data breach in 2023 that included unauthorized access to Cash App customers' data from January 1, 2023 to June 19, 2023:

> We recently identified a suspicious login to your Cash App account. At the time, we sent you an email and/or text message regarding a sign-in from a new device. We initiated an investigation and retained cybersecurity experts to assist us with the investigation to determine what happened and what data was affected. We have now

> determined that an unauthorized user logged into your Cash App account using a phone number that was linked to your account and had been recycled by your carrier. This can happen, for example, when your carrier decides a number is no longer in use by you, and the carrier gives that number to a new person.
>
> [Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Your Social Security number and driver's license information were also NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**
>
> [Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. While your Social Security number [and brokerage account number] are also contained in your Cash App account, we have no evidence this information was accessed or downloaded. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**
>
> [Your name, [Cash App account number and routing number], Cash App Card number, expiration date, and CVV appear to have been [downloaded/accessed] [on or about [date]]. While your brokerage account number is also contained in your Cash App account, we have no evidence this information was accessed or downloaded. **Your external personal bank account or card information that you connected to Cash App were NOT affected. Your Social Security number and driver's license information were NOT affected. Given that we have canceled the card, there is no ongoing risk that this card may be used fraudulently in the future.]**

64. This notice was issued at least six (6) months after the initial unauthorized access in this data breach had allegedly occurred, and Block offered no explanation as to why they had

let bad actors have a six (6) month head start on Plaintiffs and Class Members who needed to protect their PII. This caused unnecessary damages and harm to Plaintiffs and the Class.

65. Defendants failed to discover and provide timely notice and when notice was issued, it was woefully insufficient. Defendants' notice failed to provide basic details including how the Second Data Breach was discovered.

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

67. Plaintiffs' 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.

68. The Second 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.

69. Defendants disregarded the rights of Plaintiffs 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 Plaintiffs' and the Class's PII was safeguarded from access by former employees. As a result, the PII of Plaintiffs and the Class was compromised through unauthorized access resulting in damage to Plaintiffs and the Class. Plaintiffs and the Class have a continuing interest in protecting their PII.

Unauthorized Access to and Takeovers of Defendant's Users' Accounts and Impact to Users

70. Plaintiffs' counsel received numerous submissions indicating injuries to Cash App's users. Some specifically referenced the Data Breaches while others complained of the

security of Cash App more generally. These submissions indicate that potential class members' accounts were accessed without authorization and/or used by unauthorized actors, and that class members had their money taken from their accounts, that their stolen funds were not refunded or were only partially refunded, that their account experienced technical issues, that their data associated with their Cash App account was used in various unauthorized ways, or that Defendants had failed to respond appropriately or timely to their reports of unauthorized access or use by unauthorized actors.

71. Many of the potential class members' submissions indicate that they lost as much as $40,000.00 from their Cash App accounts. These funds were stolen in a plethora of different ways. This includes dozens of claims that their stolen funds were used to buy Bitcoin. In addition, unauthorized funds were used to buy Uber transactions, items on the Google marketplace, gift cards, items on the Roboblox marketplace, stocks or were given to unknown users on Cash App.

72. The stolen funds occurred at various intervals. Some Class Members submitted that the funds were only taken once while many report that the funds were taken from their account multiple times even as many as on 75 different occasions. This includes submissions that state the funds were taken from their account over long periods of time up to about a year.

73. Many of the potential Class Members submitted that money had been taken from their accounts. Potential Class Members submitted that they reached out to Cash App for assistance. Cash App in most of the submissions provided no assistance at all. Most of the submissions indicate that the Cash App denied claims for assistance and did not provide them with a refund. Some of the potential Class Members indicated in their submission that they received a refund, but it was not the full amount of the monies they had lost. One potential Class Member indicated that even after they informed Cash App that their account had been compromised, money

continued to be taken from their account. A few potential Class Members noted that Cash App allowed enough funds to be stolen from their accounts that they were left with negative balances of as much as $5,800.

74. The potential Class Members submitted the importance of the funds that were stolen from them. Many indicated the funds were necessary for rent payments, food, and other essential obligations. Others indicated that their lost funds in their Cash App account were a product of tax returns, stimulus checks, and military disability pay.

75. Following the First Data Breach, a number of potential Class Members' indicated in their submissions that they experienced technical difficulties with their Cash App account. These difficulties include locked or closed accounts with remaining balances, as well as unauthorized requests from their accounts to their contacts, including family members, for funds. One potential Class Member reported that they made a deposit into their Cash App account that never appeared in their balance and was never refunded. Another potential Class Member indicated that after their funds were taken, the fraudulent charges were deleted from their account but that the money was never refunded to them.

76. Many of the submissions also indicated that potential Class Members had their data stolen. Potential Class Members reported finding their information including names, addresses, e-mail addresses, and bank accounts on the dark web. Other potential Class Members submitted that their credit card information and social security numbers were hacked. Potential Class Members indicated that their bank accounts and credit cards were locked, in addition to unauthorized charges. One potential Class Member indicated that they were denied a credit card because of the activity following the First Data Breach. Another potential Class Member submitted that even after they were provided a new credit card the fraudulent charges continued.

77. Finally, potential Class Members submitted that they had issues with their e-mail accounts being hacked after the First Data Breach. One potential Class Member even indicated that they received threats from the individual that hacked their e-mail account.

78. The following are a small sample of over 1,000 submissions from potential Class Members:

- "I had money stolen from my cash app through Bitcoin. It was close to 3000. Cash app verified that my account was hacked and did not return my funds. After they said my account was compromised I have emails And screenshots of my cash app"
- "Cash app data breach lost most of my taxes never spent…, over 25 Uber transactions was allowed didn't authorize or have connections to"
- "Money was taking out of my account when my card was locked"
- "My cash app was deleted and my money was taken and there is no explanation on how or why"
- "I am interested in getting legal justice from Cash app. I had 1100 dollars taken from them"
- "My cashapp was hacked and $1400 was removed from my cashapp balance on February 23, 2023. I received an email from cashapp stating I requested a change of personal information, including my email. I was asked to contact them if I did authorize the change. I contacted cashapp to advise I did not authorize any changes…. The scammer has attempted to scam my family by requesting money from my mother ($200), my girlfriend ($500), and my daughter ($200) and she actually sent the funds . Fortunately, my bank refunded her the money immediately once contacted Chase have filed two separate complaints with cashapp

without any resolution or re and as of today, March 24, 2023 Cashapp is not offering any customer support and has denied my claim"

- "I had over $6,000 stole out of my cash app…"
- "I've had cashapp for now almost 3 years and they have allowed the data breach but also did not help me when my account was hacked during the breach an[d] had over $20,000 stolen during the breach as well as fraudulent transactions that cashapp will not re und or help me at all…they have caused me to lose everything"
- "My personal information was changed on my account locking me out and allowing someone else to take over my account and investments…tracked the funds to Directwealth which is cashapps brokerage there I found all the transactions. When I tried to have my other brokerage transfer all assets Directwealth gave them the run around. When they finally did allow my assets to be transferred it was only 10% what actually had in their brokerage account and money market account"
- "Cash app allowed the remainder o[f] my taxes to be taking by an unauthorized person then say [I] authorized it had almost a thousand and was left with only $17, disputed and disputed but was denied multiple times"
- "Have gotten money charged on my cash app card or fraudulent attempts, had $450.00 Disappear twice…"
- "Cash app has completely whipped out my military account stealing everything from me. I've lost my home, they cut the lights off, I'm behind on all of my bills. These people have completely destroyed my life. I am a U.S. MILITARTY VETERAN I Served my county for men and women and there families to be safe and this is how I'm treated."

- "As a user of Cash App. I have experienced issues with their trading system that have resulted in significant financial losses…"
- "Breached my data over $3650 stolen"
- "I have disputes charges and filed unauthorized charges on several occasions and never once does cashapp take responsibility for their platform and refund my money."
- "1,500 Lost to cash app Scammed from my account."
- "My cashapp that I've has since 2018-2019 has been stolen from me. It's the only account I get my child support on and I have done everything to get cashapp to get it back for me."
- "My information was compromised and some hackers were able to drain my account using my debit card number. It's plain as day that the activity is fraudulent in nature by the number of attempts to withdrawal and the varying amounts. I did my due diligence as a consumer and filed disputes on each transaction. Per Regulation E, the financial institution has 10 days to provide provisional credit; this was never completed. Lo and behold my account was terminated by Cash app for 'violation of terms.' My disputes were closed with no resolution."
- "Money was stolen from me I need some kind of help and cash app is giving me the run around . I want to take this to court."
- "Any fraudulent things that happened in my account they never side with me they always end up basically just disputing it and never give me back my money"
- "lost a ton of funds with cashapp. I've been contacting them for years still no answer"

- "My account was accessed and drained contacted Cashap within minutes and they would not do anything to recover my money"

Defendants Have Failed to Implement Reasonable Security Measures

79. 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 Plaintiffs' and the Class's PII, Defendants assumed legal and equitable duties and knew, or should have known, they were responsible for protecting Plaintiffs' and the Class's PII from unauthorized access.

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

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

82. Plaintiffs 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.

83. 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.

84. In fact, Defendants have been on notice for years that Plaintiffs' 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 Plaintiffs and the Class's PII from criminal access that Defendants anticipated (as evidenced by its Privacy Notice) and should have guarded against.

85. 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

86. 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.13

87. 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.14

88. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.15 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 computer networks;

13 *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
14 *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*].
15 *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.

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

89. 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*.

90. 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.

91. Defendants were, at all times, fully aware of their obligation to protect the PII of its users, including Plaintiffs 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.

Plaintiffs and the Class Suffered Damages

92. The ramifications of Defendants' failure to implement adequate security measures on their platform are long lasting and severe. Unauthorized access to Cash App accounts has already caused harm to users and Cash App has not sufficiently remedied those harms that have occurred. In addition, for Plaintiffs and Class Members with stolen PII, once PII is stolen, fraudulent use of that information and damage to victims may continue for years.16

16 *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

93. Accounts belonging to Plaintiffs and Class Members are private, sensitive in nature, and were left inadequately protected by Defendants who did not obtain Plaintiffs or Class Members' consent to disclose PII or permit account access to any other person as required by applicable law and industry standards.

94. Defendants required Plaintiffs 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 accounts belonging to Cash App users and the information available in those accounts was kept safe.

95. Plaintiffs 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 their accounts safe.

96. The Data Breaches and unauthorized account access were a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII and accounts 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 Plaintiffs' and Class Members' PII and accounts; and (c) protect against reasonably foreseeable threats to the security or integrity of PII and accounts.

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

98. Defendants had the resources necessary to prevent the Data Breaches and unauthorized account access, but neglected to implement adequate data security measures, despite its obligations to protect customers' PII and accounts, and despite its Privacy Notice.

99. 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 intrusions leading to the theft of PII and the unauthorized access to and transactions within accounts.

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

101. 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."17

102. As a direct result of the Defendants' failures to implement adequate security measures, Plaintiffs 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. Unauthorized account transactions;

17 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.

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

d. 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 Breaches and unauthorized access, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

e. The continued risk to their PII and accounts, which remain in the possession of Defendants and are subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in its possession and Cash App accounts; and

f. 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 Breaches and unauthorized access for the remainder of the lives of Plaintiffs and Class Members.

103. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PII and accounts are secure, remain secure, and are not subject to further unauthorized access, misappropriation and theft.

104. Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members. When Plaintiffs and Class Members have complained, Defendants' processes for resolving complaints have been inadequate and many complaints have not been resolved.

105. Defendants' failure to adequately protect Plaintiffs' and Class Members' PII and accounts has resulted in Plaintiffs 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 Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

106. 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.[18] Although their PII was improperly exposed in or about December 2021, affected current and former employees were not notified of the First Data Breach until a year later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the First Data Breach. As a result of Defendants' delay in detecting and notifying customers of the First Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

107. Similarly, Defendants' decision to notify users of the Second Data Breach months after it began has heightened Class Members' vulnerability to fraud.

V. CLASS ALLEGATIONS

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

18 *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.

> **Nationwide Class:** All persons who are current or former customers of Defendants or any of Defendants' affiliates, parents, or subsidiaries and who had their PII, Cash App account, or Cash App Investing account accessed or obtained without their authorization or who otherwise had unauthorized, unintended or fraudulent withdrawals or transfers to or from, or alleged error in connection with, a Cash App or Cash App Investing account or any linked financial account.

In addition, Plaintiffs bring this action on behalf of the following proposed subclasses defined as follows:

> **Texas Subclass:** All persons residing in the State of Texas who are current or former customers of Defendants or any of Defendants' affiliates, parents, or subsidiaries and who had their PII, Cash App account, or Cash App Investing account accessed or obtained without their authorization or who otherwise had unauthorized, unintended or fraudulent withdrawals or transfers to or from, or alleged error in connection with, a Cash App or Cash App Investing account or any linked financial account.

> **Illinois Subclass:** All persons residing in the State of Illinois who are current or former customers of Defendants or any of Defendants' affiliates, parents, or subsidiaries and who had their PII, Cash App account, or Cash App Investing account accessed or obtained without their authorization or who otherwise had unauthorized, unintended or fraudulent withdrawals or transfers to or from, or alleged error in connection with, a Cash App or Cash App Investing account or any linked financial account.

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

110. 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.

111. **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.

112. **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 Plaintiffs and the other Class Members' PII;

c. Whether Defendants owed a legal duty to Plaintiffs 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 Plaintiffs and the Class Members to prevent fraud on Cash App and to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Defendants error resolution processes were inadequate;

f. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breaches;

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

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

i. Whether Defendants have engaged in fraud;

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

k. Whether Plaintiffs and the other Class Members have suffered damages as a result of unauthorized access to their accounts and deficiencies in Cash App's error resolution processes;

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

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

113. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs 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.

114. **Typicality.** Plaintiffs' 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.

115. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because her interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

116. **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 Plaintiffs 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 Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

117. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

118. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs and Class Members' financial accounts and PII from being compromised, lost, stolen, and accessed by unauthorized persons and in responding to complaints of unauthorized access and other account errors. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs and Class Members' accounts and PII in Defendants' possession were adequately secured and protected.

119. Defendants owed a duty of care to Plaintiffs 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.

120. Defendants owed a duty of care to Plaintiffs 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.

121. Plaintiffs and Class Members entrusted Defendants with their financial accounts and PII with the understanding that Defendants would safeguard them, that Defendants would not store their PII longer than necessary, and that Defendants were capable of protecting against the harm suffered by Plaintiffs and Class Members.

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

123. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their financial accounts and PII. Defendants' misconduct included failing to implement the necessary systems, policies, employee training, and procedures necessary to prevent the Data Breaches and protect financial accounts.

124. Defendants knew, or should have known, of the risks inherent in maintaining financial accounts for consumers and 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.

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

126. Plaintiffs' injuries and damages, as described below, are a reasonably certain consequence of Defendants' breach of its duties.

127. 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 and consumer financial accounts contained therein.

128. Plaintiffs and Class Members reasonably believed that Defendants would take adequate security precautions to protect their PII and financial accounts. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs and Class Members' PII.

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

130. 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.

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

132. 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 and error resolution procedures and practices, Plaintiffs and Class Members

have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) unauthorized or unintended transactions associated with their Cash App accounts that were not appropriately resolved; (ii) the loss of the opportunity to determine for themselves how their PII is used; (iii) the publication and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports and password protection; (vii) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (viii) 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 (ix) 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.

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

a. The harm caused to the Plaintiffs and the Class was foreseeable. Defendants maintained financial accounts of the Plaintiffs and the Class and collected their

PII. Defendants understood that injury would occur to Plaintiffs and the Class if their financial accounts and PII were not adequately protected and that a data breach would damage its current and former customers.

b. Defendants' services were intended to affect Plaintiffs 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 Plaintiffs and the Class Members. Plaintiffs and the Class Members were specifically targeted by Defendants. By virtue of Defendants' services, Defendants intended to affect Plaintiffs 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 Plaintiffs and Class Members. The Plaintiffs and Class Members suffered the following injuries:

    i. unauthorized or unintended transactions associated with their Cash App accounts;

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

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

    iv. out-of-pocket expenses associated with the prevention, detection, and

recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time;

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

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

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

viii. 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

ix. 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 Plaintiffs 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 Plaintiffs' and Class Member's PII, as evidenced by the Data Breaches; 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 Plaintiffs and the Nationwide Class or, alternatively, the Texas Subclass)

134. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

135. 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 Plaintiffs 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.

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

137. 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 Plaintiffs and the other members of the class.

138. 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.

139. 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.

140. Defendants stored the PII of Plaintiffs 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.

141. Defendants knew or should have known that it did not employ reasonable measures to keep the PII or financial information of Plaintiffs 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.

142. Defendants' deceptive acts and business practices induced Plaintiffs and the Class Members to use its app and to provide their PII. But for these deceptive acts and practices, Plaintiffs and the other Class Members would not have provided their PII to Defendants or utilized its services. If Defendants had disclosed the security inadequacies, Plaintiffs 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.

143. Plaintiffs 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. Plaintiffs 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. Plaintiffs 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.

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

145. Pursuant to CLRA, Plaintiffs 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 Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

146. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

147. 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 Plaintiffs and the class. Defendants were also aware that many of their users were experiencing hacking incidents on its platform.

148. 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 Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs and Class Members' financial accounts and 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 Plaintiffs, Class Members, and the Defendants, Defendants had a duty to disclose to Plaintiffs and Class Members that its security system did not have the robust measures needed to adequately protect the PII it required Plaintiffs and Class Members to provide.

149. 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.

150. Plaintiffs and the class relied on Defendant's inadequate disclosures by utilizing its platform. Had Plaintiffs 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.

151. As a result of the foregoing, Plaintiffs and the Class sustained damages as alleged herein. Plaintiffs and the Class Members suffered unauthorized transactions that were not resolved and diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs 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 Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

152. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

153. 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 First 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 Plaintiffs and the class or warn them.

154. 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.

155. Instead, Defendants did not make this disclosure. Defendants willfully deceived Plaintiffs 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 regulatory guidelines, coupled with its contemporaneous knowledge of repeated hacking incidents occurring among its users, evidences Defendants' duty to disclose additional material facts.

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

157. 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.

158. As a result of this deceit by Defendants, Defendants are liable under Cal. Civ. Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer []." Because of Defendants' deceit, (1) the PII and financial information of Plaintiffs and the Class was compromised, placing them at a greater risk of identity theft; (2) Plaintiffs and the Class were subjected to identity theft; (3) Plaintiffs and the Class's PII was accessed by a third party, without their consent (4) Plaintiffs 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) Plaintiffs 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.

159. 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, Plaintiffs 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 Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

160. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

161. 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.

162. 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.

163. 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 the Data Breaches, nor would it have been subject to prior hacking incidents as specified above.

164. 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.

165. Defendant made this assertion with the intent that Plaintiffs 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 Plaintiffs' and the Class's reliance. By making these negligent misrepresentations Defendant intended for Plaintiffs 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 Plaintiffs and Class Members would rely on this representation to their detriment and utilize its services.

166. Plaintiffs and the Class were unaware of the falsity of Defendants' representation, otherwise they would not have utilized Defendants' services. Plaintiffs 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. Plaintiffs justifiably relied on this representation because the application was well-known and used by many other Americans.

167. As a result of Plaintiffs' and the Class Members' reliance on the Defendants' negligent misrepresentations, Plaintiffs and the Class Members sustained damages in the form of their PII being exploited, misused, and stolen. This is evidenced by the Data Breaches.

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

COUNT SIX
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

169. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

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

171. As a condition of its services, Defendants required Plaintiffs 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 Plaintiffs and Class Members in its possession were only used to provide the agreed-upon benefits from Defendants.

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

173. These agreements were made by Plaintiffs or Class Members who were customers of Defendants.

174. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs 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 Plaintiffs and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with services and benefits.

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

176. Plaintiffs 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.

177. Plaintiffs 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.

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

179. Defendants' failure to implement adequate measures to protect the PII of Plaintiffs

and Class Members violated the purpose of the agreement between the parties.

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

181. Instead of spending adequate financial resources to safeguard Plaintiffs and Class Members' PII, which Plaintiffs 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 Plaintiffs and Class Members.

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

COUNT SEVEN
Breach of Confidence
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

183. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

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

185. Plaintiffs and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiffs 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.

186. As alleged herein and above, Defendants' relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

187. Plaintiffs 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.

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

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

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

191. But for Defendants' disclosure of Plaintiffs 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 Breaches were the direct and legal cause of the theft of Plaintiffs and Class Members' PII, as well as the resulting damages.

192. This disclosure of Plaintiffs and Class Members' PII constituted a violation of

Plaintiffs and Class Members' understanding that Defendants would safeguard and protect the confidential and novel PII that Plaintiffs and Class Members were required to disclose to Defendants.

193. The concrete injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs and Class Members' PII. Defendants knew its data security procedures for accepting and securing Plaintiffs and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiffs and Class Members' PII in jeopardy.

194. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs 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 Breaches, 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 Breaches for the remainder of the lives of Plaintiffs and Class Members.

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

195. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

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

197. 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).

198. In addition, Defendants are required to create an "accountability program" and use due diligence in engaging a third party to process 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.*

199. 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.

200. Plaintiffs 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.

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

202. 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.

203. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiffs and Class Members that was private and is entitled to remain private. Plaintiffs 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. Plaintiffs 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 Breaches, which were caused by Defendants' negligent actions and inactions, constitutes an intentional interference with Plaintiffs 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.

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

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

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

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

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

209. As a proximate result of Defendants' acts and omissions, Plaintiffs 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 Plaintiffs and Class Members to suffer concrete damages as described herein.

210. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs 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.

211. Plaintiffs 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 Plaintiffs and Class Members.

COUNT NINE
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

212. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

213. In light of its special relationship, Defendants became the guardian of Plaintiffs 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 Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs and Class Members' PII and to timely detect and notify them in the event of a data breach.

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

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

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

217. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs 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 Breaches, 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 Plaintiffs' 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 Breaches for the remainder of the lives of Plaintiffs and Class Members.

218. As a direct and proximate result of Defendants' breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT TEN
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Subclasses)

219. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

220. As described above, when Plaintiffs 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 Plaintiffs and Class Members' PII and to timely detect and notify them in the event of a data breach.

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

222. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs 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 Plaintiffs and Class Members' PII if it did not intend to provide Plaintiffs and Class Members services and to receive financial benefits in return.

223. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs 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.

224. Plaintiffs 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.

225. 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.

226. 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 Plaintiffs 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 Plaintiffs 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.

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

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

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

230. Plaintiffs 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.

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

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

COUNT ELEVEN
Declaratory and Injunctive Relief
(On behalf of Plaintiffs and Nationwide Class or, alternatively, the Subclasses)

233. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

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

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

236. Defendants owe a duty of care to Plaintiffs and Class Members requiring Defendants to secure their PII and accounts and respond appropriately to reports of unauthorized access and transactions.

237. Defendants still possess PII regarding Plaintiffs and Class Members.

238. Since the First 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 Breaches to occur and, thereby, prevent future attacks.

239. Defendants have not satisfied its contractual obligations and legal duties to Plaintiffs 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.

240. Actual harm has arisen regarding Defendants' contractual obligations and duties of care to provide security and response measures to Plaintiffs and Class Members. Further, Plaintiffs 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.

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

242. Plaintiffs, 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 comply with statutory and regulatory error resolution procedures;

j. 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

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

243. Plaintiffs Salinas and Gordon incorporate the foregoing paragraphs as if fully set forth herein.

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

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

246. Plaintiffs 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.

247. 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.

248. 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.*

249. By failing to disclose prior hacking incidents and concealing the defective nature of the App's security features from Plaintiffs 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.

250. 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.

251. 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.

252. Defendant was under a duty to Plaintiffs 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. Plaintiffs 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 Plaintiffs 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.

253. The facts concealed or not disclosed by Defendant to Plaintiffs 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.

254. Plaintiffs 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.

255. 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.

256. Moreover, Defendants' 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 Plaintiffs 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 Plaintiffs and the Texas Subclass.

257. The facts concealed or not disclosed by Defendant to Plaintiffs 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.

258. Had Plaintiffs and other Texas Subclass Members known that the App had inadequate security features and had been the target of prior hacking instances and that Defendants did not respond appropriately to reports of such issues, they would not have utilized CashApp or would have taken other precautions to protect their PII.

259. Plaintiffs 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.

260. As a result of Defendants' misconduct, Plaintiffs and the other Class Members have been harmed and have suffered actual and economic damages. Plaintiffs and the other Class Members PII was compromised, placing them at a greater risk of identity theft. Plaintiffs 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. Plaintiffs 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.

261. Plaintiffs has mailed a letter to Defendants, pursuant to V.T.C.A., Bus. & C. Code § 17.505, giving written notice of the action.

COUNT THIRTEEN

Violation of California's Unfair Competition Law ("UCL"),
Cal. Bus. Prof. Code § 17200, *et seq.*,
(On Behalf of Plaintiffs and the Nationwide Class)

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

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

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

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

c. By failing to prevent unauthorized transactions and unauthorized access to accounts that were accessed without authorization and/or used by unauthorized actors;

d. By failing to comply with statutory error resolution procedures such as those found in the Electronic Fund Transfer Act and its implementing regulations; and

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

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

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

266. Defendants knew or should have known that their administrative and data security measures were inadequate to safeguard Plaintiffs' and Class members' Private Information and that the risk of a data breach or unauthorized access to consumer financial accounts was highly

likely. Defendants had resources to secure and/or prepare for protecting customers' financial accounts and Private Information in a data breach. Defendants' actions in engaging in the above-named unfair, unlawful and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

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

COUNT FOURTEEN

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CRA"), Cal. Bus. Prof. Code § 1798.80, *et seq.*, (On Behalf of Plaintiffs and the Nationwide Class)

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

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

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

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

their duty to inform their customers of unauthorized access expeditiously and without unreasonable delay.

272. The Data Breaches described herein are "breach[es] of the security system" under Section 1798.82.

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

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

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

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

COUNT FIFTEEN

VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT,
815 ILCS §§ 505, *et seq*.
(On Behalf of Plaintiff Washington and the Illinois Subclass)

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

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

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

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

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

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

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

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

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

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

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

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

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

i. Failing to prevent unauthorized transactions and unauthorized access to accounts that were accessed without authorization and/or used by unauthorized actors; and

j. Failing to comply with statutory error resolution procedures such as those found in the Electronic Fund Transfer Act and its implementing regulations.

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

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

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

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

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

287. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

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

COUNT SIXTEEN
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,
815 ILCS §§ 510/2, *et seq*.
(On Behalf of Plaintiff Washington and the Illinois Subclass)

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

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

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

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

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

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

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

292. Defendants' deceptive trade practices include:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 Plaintiffs 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 Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members;

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

v. prohibiting Defendants from maintaining Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members damages;

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

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

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

VIII. 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: February 9, 2024

Respectfully submitted,

/s/ *Nicholas A. Migliaccio*
Nicholas A. Migliaccio (admitted pro hac vice)
Jason S. Rathod (admitted pro hac vice)
MIGLICACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Telephone (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Melissa R. Emert (admitted pro hac vice)
Gary Graifman (admitted pro hac vice)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Tel: (845) 356-2570

William B. Federman (admitted pro hac vice)
FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Ph: 405-235-1560

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

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

Proposed Class Counsel

MIGLIACCIO & RATHOD LLP
Nicholas Migliaccio, *admitted pro hac vice*
Jason Rathod, *pro hac vice forthcoming*
412 H St NE #302
Washington, D.C. 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

KANTROWITZ GOLDHAMER & GRAIFMAN PC
Gary Graifman, *admitted pro hac vice*
Melissa Emert, *admitted pro hac vice*
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Tel: (845) 356-2570
ggraifman@kgglaw.com
memert@kgglaw.com

FEDERMAN & SHERWOOD
William B. Federman, *admitted pro hac vice*
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
Tel: (405) 235-1560
wbf@federmanlaw.com

Proposed Class Counsel
Additional Propose Class Counsel on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHELLE SALINAS, RAYMEL WASHINGTON, and AMANDA GORDON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

BLOCK, INC. and CASH APP INVESTING, LLC,

Defendants.

CASE NO. 3:22-cv-04823

SUPPLEMENTAL DECLARATION OF NICHOLAS A. MIGLIACCIO IN SUPPORT OF PLAINTIFFS' MOTION TO CONSOLIDATE PURSUANT TO FED. R. CIV. P. 42(A) AND FOR APPOINTMENT OF INTERIM CO-LEAD CLASS COUNSEL

I, Nicholas A. Migliaccio, hereby declare as follows:

1. In furtherance of Plaintiffs' unopposed Motion To Consolidate Pursuant to Fed. R. Civ. P. 42(a) (ECF No. 71, 72), a true and correct copy of the Proposed Consolidated Complaint is attached hereto as Exhibit A.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 9th day of February 2024 at Washington D.C.

Respectfully submitted,

/s/ *Nicholas A. Migliaccio*
Nicholas A. Migliaccio (admitted pro hac vice)
Jason S. Rathod (admitted pro hac vice)
MIGLICACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Telephone (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Melissa R. Emert (admitted pro hac vice)
Gary Graifman (admitted pro hac vice)
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Tel: (845) 356-2570

William B. Federman (admitted pro hac vice)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Ph: 405-235-1560

Daniel E. Gustafson (admitted pro hac vice)
David A. Goodwin (admitted pro hac vice)
Mary M. Nikolai (admitted pro hac vice)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600

Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
mnikolai@gustafsongluek.com

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

Proposed Class Counsel