

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

George Kattula, Ashley Adams, John Alexander, Kenneth Axelsson, Tara Bennett, Al Bigonia, Joseph Blumetti, Darren Bradley, Dallas Bray, Franklin Calderón, Wayne Colt Carter, Allan Chiulli, Lolletta Cohen, Laleh Dallalnejad, Erick Eliezaire, Mark Gambell, Rodrigo Garcia, Mark Girshovich, Charles Glackin, Eldon Hastings, Roger Haston, Travis Houzenga, Dan Hyatt, Bobby Johnson, Jane Krieser, Eric Larson, Chris Longstreth, Ngoun Mang, Lisa Marcial, Bianca McWilliams, Victor Mechanic, Mihail Mihalitsas, Brady Lee Nessler, Frank Onimus, Vilasini Pillai, William Plyler, Edward Polhill, Steven Paperno, Luis Rodriguez, Earlando Samuel, Von Sims, Varun Singh, Larry Sowell, Vesselina Spassova, Richard Stefani, Christopher Suero, Natalie Tang, Daniel Tucker, Fatima Waheed, Eric White, Bob Whittington, and Karen Wright, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

Coinbase Global, Inc., and  
Coinbase Inc.,

Defendants.

CIVIL FILE ACTION

NO. 1:22-cv-03250-TWT

**CLASS ACTION**

JURY TRIAL DEMANDED

**FIRST AMENDED COMPLAINT**

## **FIRST AMENDED COMPLAINT**

Plaintiffs, on behalf of themselves and all others similarly situated, file this Amended Class Action Complaint (“Complaint”) against Coinbase Global, Inc. and Coinbase, Inc. for declaratory judgement, injunctive relief, damages, and other equitable relief. Based upon personal knowledge of the facts pertaining to Plaintiffs and the investigation of counsel, Plaintiffs allege as follows:

### **INTRODUCTION**

1. This is a class action brought by Plaintiffs on behalf of all Coinbase users, including Coinbase account holders and Coinbase “Wallet” users, who have lost or been deprived of access to their account holdings. Coinbase has touted its platforms, services, and accounts as being the most trusted, most secure, and protected by scrupulous industry-leading bank-level security. In reality, Coinbase’s security measures for its customers’ accounts are little better than if its customers stuffed their cash in their mattresses, with the notable exception that Coinbase collects fees while negligently allowing its customers’ accounts to be looted.

2. Thousands of Coinbase customers have had their accounts looted. There is even, for example, a Facebook group with thousands of members that is entitled “Coinbase Clients Demanding Justice.”

3. Coinbase Global, Inc. is a publicly-traded corporation involved in the business of cryptocurrency exchange. Its wholly-owned subsidiary, Coinbase, Inc. (referred to herein as “Coinbase”), provides an online platform (Coinbase.com) where consumers can store their currencies in a digital “wallet,” as well as buy, sell, spend, and trade cryptocurrency on exchanges (“platform”). Coinbase also offers Coinbase Wallet (hereinafter “Coinbase Wallet” or “Wallet”).

4. Coinbase holds itself out as a regulated and fully compliant entity, registered with the United States Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) as a Money Services Business, as that term is defined by FinCEN. Coinbase also holds itself out as compliant with the Bank Secrecy Act, the USA Patriot Act, state money transmission laws, and corresponding regulations.

5. Coinbase is the largest cryptocurrency exchange based in the United States. According to Coinbase, it has “built [its] reputation on the premise that [its] platform offers customers a secure way to purchase, store, and transact in crypto assets.” In its words, what “sets [Coinbase] apart” from competitors is that its “custom technology platform is built to deal with the real-time, global and 24/7/365 nature of the crypto asset markets . . .”

6. Contrary to its representations, which are designed to induce consumers to entrust Coinbase with funds, Coinbase does not properly employ standard practices to safeguard and protect user accounts on Coinbase.com or Coinbase Wallets. The Coinbase exchange (Coinbase.com) and Coinbase Wallet are riddled with security flaws. Further, Coinbase improperly and unreasonably locks out its consumers from accessing their accounts and funds, either for extended periods of time or indefinitely.

7. Making matters worse, Coinbase (or its outsourced customer service) fails to timely respond to customer pleas for support, requests to secure an account, or requests to access an account. When Coinbase does respond, it sends customers into an endless, vicious cycle of automated email responses as part of its months-long sham dispute resolution process. Because of the extreme volatility of cryptocurrencies' value – with freefalls of 40% within 24 hours not unheard of – the inability to access an account to sell, buy, or trade cryptocurrency leads to severe financial loss to account holders.

8. Coinbase's failures have prevented Plaintiffs and Class Members from having "full control of [their] crypto" and from being able to "invest, spend, save, earn, and use," or withdraw their funds as Coinbase promises.

9. As a result of Coinbase's conduct, Plaintiffs and Class Members have been damaged through the loss of access to their wallets/accounts, loss of information associated with their wallets/accounts, loss of the funds and cryptocurrencies in those wallets/accounts, and, among other things, loss of their investment opportunities.

10. Accordingly, Plaintiffs seek damages and equitable relief on behalf of themselves and those similarly situated, as well as declaratory relief that (1) Coinbase's class action waiver provisions are unenforceable as a matter of law; and (2) Coinbase's onerous arbitration provisions, including the delegation clause purportedly determining the scope of the arbitrator's authority, are procedurally and substantively unconscionable and unenforceable as against Plaintiffs and the Class Members. Plaintiffs also seek actual damages, statutory damages, punitive damages, restitution, and all applicable interest thereon, along with attorneys' fees, costs, and expenses; as well as injunctive relief, including significant improvements to Coinbase's data security systems and protocols (which have been the subject of successive data breaches), future annual audits, Coinbase-funded long-term credit monitoring services, and any other remedies the Court deems necessary and proper, up to and including the appointment of a corporate monitor.

**PLAINTIFFS**

11. Plaintiffs bring this action on behalf of themselves, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

12. Plaintiffs are former and also current users of Coinbase’s services or products, including Coinbase accounts, Coinbase Pro accounts, and the Coinbase Wallet. Plaintiffs have suffered injuries from Coinbase’s lax security measures and inadequate customer support.

**Alabama**

13. Plaintiff Eric White (“Mr. White”) is a resident of the state of Alabama and has been an Alabama resident at all times relevant to this Complaint.

**Arizona**

14. Plaintiff Richard Stefani (“Mr. Stefani”) is a resident of the state of Arizona and has been an Arizona resident at all times relevant to this Complaint.

15. Plaintiff Eldon Hastings (“Mr. Hastings”) is a resident of the state of Arizona and has been an Arizona resident at all times relevant to this Complaint.

16. Plaintiff Jane Krieser (“Ms. Krieser”) is a resident of the state of Arizona and has been an Arizona resident at all times relevant to this Complaint.

17. Plaintiff Bianca McWilliams (“Ms. McWilliams”) is a resident of the state of Arizona and has been an Arizona resident at all times relevant to this Complaint.

18. Plaintiff Mark Gambell (“Mr. Gambell”) is a resident of the state of Arizona and has been an Arizona resident at all times relevant to this Complaint.

### **California**

19. Plaintiff Natalie Tang (“Ms. Tang”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

20. Plaintiff Darren Bradley (“Mr. Bradley”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

21. Plaintiff Bob Whittington (“Mr. Whittington”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

22. Plaintiff Von Sims (“Mr. Sims”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

23. Plaintiff Varun Singh (“Mr. Singh”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

24. Plaintiff Laleh Dallalnejad (“Ms. Dallalnejad”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint.

25. Plaintiff Charles Glackin (“Mr. Glackin”) is a resident of the state of California and has been a California resident at all times relevant to this Complaint

**Florida**

26. Plaintiff Frank Onimus (“Mr. Onimus”) is a resident of the state of Florida and has been a Florida resident at all times relevant to this Complaint.

27. Plaintiff Erick Eliezaire (“Mr. Eliezaire”) is a resident of the state of Florida has been a Florida resident at all times relevant to this Complaint.

28. Plaintiff Larry Sowell (“Mr. Sowell”) is a resident of the state of Florida and has been a Florida resident at all times relevant to this Complaint.

29. Plaintiff Christopher Suero (“Mr. Suero”) is a resident of the state of Florida has been a Florida resident at all times relevant to this Complaint.

30. Plaintiff Luis Rodriguez (“Mr. Rodriguez”) is a resident of the state of Florida has been a Florida resident at all times relevant to this Complaint.

31. Plaintiff Eric Larson (“Mr. Larson”) is a resident of the state of Florida has been a Florida resident at all times relevant to this Complaint.



32. Plaintiff Dallas Bray (“Mr. Bray”) is a resident of the state of Florida has been a Florida resident at all times relevant to this Complaint.

### **Georgia**

33. Plaintiff George Kattula (“Mr. Kattula”) is a resident of the state of Georgia and has been a Georgia resident at all times relevant to this Complaint.

34. Plaintiff Kenneth Axelsson (“Mr. Axelsson”) is a resident of the state of Georgia and has been a Georgia resident at all times relevant to this Complaint.

35. Plaintiff Roger Haston (“Mr. Haston”) is a resident of the state of Georgia and has been a Georgia resident at all times relevant to this Complaint.

36. Plaintiff Lolletta Cohen (“Ms. Cohen”) is a resident of the state of Georgia and has been a Georgia resident at all times relevant to this Complaint.

37. Plaintiff Rodrigo Garcia (“Mr. Garcia”) is a resident of the state of Georgia and has been a Georgia resident at all times relevant to this Complaint.

38. Mr. Kattula, Mr. Axelsson, Mr. Haston, Ms. Cohen, and Mr. Garcia are collectively referred to as the “Georgia Plaintiffs.”

### **Illinois**

39. Plaintiff Daniel Tucker (“Mr. Tucker”) is a resident of the state of Illinois and has been an Illinois resident at all times relevant to this Complaint.

40. Plaintiff Vesselina Spassova (“Ms. Spassova”) is a resident of the state of Illinois and has been an Illinois resident at all times relevant to this Complaint.

41. Plaintiff Travis Houzenga (“Mr. Houzenga”) is a resident of the state of Illinois and has been an Illinois resident at all times relevant to this Complaint.

42. Plaintiff Fatima Waheed (“Ms. Waheed”) is a resident of the state of Illinois and has been an Illinois resident at all times relevant to this Complaint.

### **Louisiana**

43. Plaintiff Ashley Adams (“Ms. Adams”) is a resident of the state of Louisiana and has been a Louisiana resident at all times relevant to this Complaint.

### **Michigan**

44. Plaintiff Edward Polhill (“Mr. Polhill”) is a resident of the state of Michigan and has been a Michigan resident at all times relevant to this Complaint.

### **New Hampshire**

45. Plaintiff Al Bigonia (“Mr. Bigonia”) is a resident of the state of New Hampshire and has been a New Hampshire resident at all times relevant to this Complaint.

### **New Jersey**

46. Plaintiff Mark Girshovich (“Mr. Girshovich”) is a resident of the state of New Jersey and has been a New Jersey resident at all times relevant to this Complaint.

47. Plaintiff Vilasini Pillai (“Ms. Pillai”) is a resident of the state of New Jersey and has been a New Jersey resident at all times relevant to this Complaint.

### **New York**

48. Plaintiff Mihail Mihalitsas (“Mr. Mihalitsas”) is a resident of the state of New York and has been a New York resident at all times relevant to this Complaint.

### **Ohio**

49. Plaintiff Chris Longstreth (“Mr. Longstreth”) is a resident of the state of Ohio and has been an Ohio resident at all times relevant to this Complaint.

50. Plaintiff Joseph Blumetti (“Mr. Blumetti”) is a resident of the state of Ohio and has been an Ohio resident at all times relevant to this Complaint.

### **Oklahoma**

51. Plaintiff Wayne Colt Carter (“Mr. Colt Carter”) is a resident of the state of Oklahoma and has been a Oklahoma resident at all times relevant to this Complaint.

### **Oregon**

52. Plaintiff Dan Hyatt (“Mr. Hyatt”) is a is a resident of the state Oregon and has been an Oregon resident at all times relevant to this Complaint.

### **Pennsylvania**

53. Plaintiff Lisa Marcial (“Ms. Marcial”) is a resident of the state of Pennsylvania has been a Pennsylvania resident at all times relevant to this Complaint.

54. Plaintiff William Plyler (“Mr. Plyler”) is a resident of the state of Pennsylvania has been a Pennsylvania resident at all times relevant to this Complaint.

55. Plaintiff Earlando Samuel (“Mr. Samuel”) is a resident of the state of Pennsylvania has been a Pennsylvania resident at all times relevant to this Complaint.

### **Tennessee**

56. Plaintiff John Alexander (“Mr. Alexander”) is a resident of the state of Tennessee and has been a Tennessee resident at all times relevant to this Complaint.

57. Plaintiff Brady Lee Nessler (“Mr. Nessler”) is a resident of the state of Tennessee and has been a Tennessee resident at all times relevant to this Complaint.

### **Texas**

58. Plaintiff Allan Chiulli (“Mr. Chiulli”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

59. Plaintiff Tara Bennett (“Ms. Bennett”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

60. Plaintiff Franklin Calderón (“Mr. Calderón”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

61. Plaintiff Bobby Johnson (“Mr. Johnson”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

62. Plaintiff Steven Paperno (“Mr. Paperno”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

63. Plaintiff Karen Wright (“Ms. Wright”) is a resident of the state of Texas and has been a Texas resident at all times relevant to this Complaint.

### **Washington**

64. Plaintiff Ngoun Mang (“Mr. Mang”) is a resident of the state of Washington and has been a Washington resident at all times relevant to this Complaint.

### **Wisconsin**

65. Plaintiff Victor Mechanic (“Mr. Mechanic”) is a resident of the state of Wisconsin and has been a Wisconsin resident at all times relevant to this Complaint.

### **DEFENDANTS**

66. Defendant Coinbase Global, Inc. (“Coinbase Global”) is a publicly-traded Delaware corporation that is involved in the business of cryptocurrency exchange, among other interrelated businesses. Defendant Coinbase Global operates worldwide on a virtual platform and claims not to have a formal physical headquarters since it is a “remote first” company. Also, a wholly owned subsidiary of Coinbase Global, the Singapore private limited company Toshi Holdings Pte. Ltd., developed and makes available to users the Coinbase Wallet.

67. Defendant Coinbase, Inc. (“Coinbase”), a Delaware corporation, is a wholly owned subsidiary of Coinbase Global, Inc. Coinbase Global and Coinbase, Inc. are operated as one corporation. Coinbase Global maintains its executive offices in San Francisco, California, which are shared with Defendant Coinbase, Inc. Coinbase Global’s SEC filings refer to Coinbase Global and Coinbase, Inc. (together with other subsidiaries of Coinbase Global) as “the Company” or “Coinbase.” The founder of Coinbase, Brian Armstrong, is the CEO of both Coinbase and Coinbase Global. Users have little or no visibility into which entity they are transacting with.

**JURISDICTION AND VENUE**

68. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The aggregate amount-in-controversy, exclusive of costs and interests, exceeds the sum of \$5,000,000.00, as there are well over 100 members of the Class, and this is a class action in which at least one member of the proposed class is a citizen of a state different than Defendants.

69. Pursuant to 28 U.S.C. § 1331, this Court also has federal question subject matter jurisdiction because this Complaint asserts claims under the Electronic Funds Transfer Act, 15 U.S.C. § 1693.

70. The Court has supplemental jurisdiction over Plaintiffs' state-law claims pursuant to 28 U.S.C. § 1367.

71. This Court has personal jurisdiction over Defendants because, under the provisions of O.C.G.A. §§ 7-1-680 et seq., Coinbase, Inc. is licensed by the State of Georgia Department of Banking and Finance, to engage in the business of Selling Payment Instruments. See GA LICENSE# 42796 NMLS# 1163082. Coinbase, Inc. also routinely conducts business in Georgia, has sufficient minimum contacts in Georgia, and has intentionally availed itself of this jurisdiction by marketing and selling products and services in Georgia. Coinbase also holds itself out as a “remote-

first” company with employees working throughout the United States and in Georgia.

72. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant Coinbase, Inc. conducts a substantial amount of its business in this District, and some of the events that give rise to several of Plaintiffs’ claims occurred in this District.

73. Defendants’ conduct as alleged herein has had a substantial effect on interstate and intrastate commerce. At all material times, Defendants participated in the conduct set forth herein in a continuous and uninterrupted flow of commerce across state and national lines and throughout the United States.

## **FACTUAL ALLEGATIONS**

### **I. Background on Coinbase**

74. Coinbase offers an online platform for purchasing, holding, and transferring title to cryptocurrency.

75. Coinbase has over 100 million users, in over 100 countries, with \$309 billion of cryptocurrency traded quarterly. As of March 31, 2022, customers entrusted Coinbase’s platform with approximately \$256 billion in fiat currency and cryptocurrency assets. In September 2022, Coinbase.com declared: “Over 103 million people and businesses trust us to buy, sell, and manage crypto.”



76. Coinbase has not registered as either a securities exchange or as a broker-dealer.

77. In addition to providing a cryptocurrency exchange, Coinbase provides a “custodial-wallet” for holding cryptocurrency and has participated in the issuance of a prominent digital currency, a so-called “stablecoin,” that is tied to the value of the U.S. dollar.

78. Coinbase account holders can use their accounts to buy, sell, spend, and trade cryptocurrency, such as Bitcoin. Coinbase explains that assets held in its accounts often are easily used for consumer payments.<sup>1</sup> Coinbase users may even obtain a debit card to use in connection with their account.

79. In recent years, Coinbase experienced tremendous growth. The company grew from 199 employees as of December 31, 2017, to 1,717 employees by March 31, 2021, approximately 40% of which work in engineering, product, and design teams. Its net income catapulted from a loss of \$30.4 million in 2019 to positive net income of \$3.6 billion in 2021. Its number of monthly transacting users – retail users who make at least one transaction during a given 28-day period – surged from approximately one million per month at the end of 2019 to

---

<sup>1</sup> <https://help.coinbase.com/en/coinbase/getting-started/crypto-education/where-can-i-spend-bitcoin>.

approximately 11.4 million two years later, an over 1,000% increase. Its total number of verified users grew similarly – from a total of approximately 32 million users in 2019 to approximately 98 million users as of March 2022.

80. Coinbase’s user growth has drastically outpaced its ability to provide the account services and protections it promises to consumers, leaving consumers, their funds and their accounts vulnerable.

81. Before Plaintiffs’ experiences with Coinbase, Coinbase was aware it was woefully incapable, understaffed, and overstretched, such that it could not perform its promises and obligations to consumers like Plaintiffs. By 2018, Coinbase’s customers had submitted at least 134 pages of complaints to the U.S. Securities and Exchange Commission and the California Department of Business Oversight. The Consumer Financial Protection Bureau’s database of consumer complaints reports there are over 5,700 complaints against Coinbase, including over 1,000 such complaints in the last year alone.

82. As another example, in 2019, a Minnesota consumer’s Coinbase account was locked due to unauthorized attempts to access it. It took Coinbase **six months** to conduct a security investigation and restore access to that consumer. *See In the Matter of Coinbase, Inc. License No. MN-MT-1153082.*

83. When Coinbase users (or thieves) make transactions, Coinbase collects fees for the transactions. Coinbase earns the vast majority of its income, approximately \$1.2 billion for the quarter ending March 31, 2022, through fees generated primarily from account transactions. It also earns interest on U.S. currency held in customer accounts.

84. Coinbase claims it pools the U.S. currency held in customers' accounts and places such funds in FDIC insured bank accounts and/or purportedly invests them in liquid investments. Coinbase keeps the interest and earnings from those funds for itself. According to Coinbase, this makes cash held with Coinbase insured by the FDIC up to the FDIC's coverage limit, which is currently \$250,000 per depositor, per insured bank, for each account ownership category.

85. Coinbase advertises that eligible users can transfer a portion of their paycheck or the entire paycheck to their Coinbase Account. Coinbase states it "has partnered with MetaBank®, N.A. to offer the Coinbase Direct Deposit product" and paychecks are "deposited and accepted by our bank partner, MetaBank®, N.A.," a ". . . Member FDIC . . ."

86. Plaintiffs and the other members of the Class reasonably believed that Coinbase would provide the safe, secure, and easy-to-access platform it promised.

Plaintiffs and the Class also reasonably believed their assets and funds were safe and protected.

87. Plaintiffs, like the other Class Members they seek to represent, have a Coinbase Wallet or Coinbase account hosted by Coinbase that purportedly enables them to conduct transactions in cryptocurrency 24 hours a day, 7 days a week and 365 days a year. Each Coinbase user account should reflect those transactions and permit access to their cash, cryptocurrencies, and other funds. Accordingly, Plaintiffs and all account holders are entitled to, reasonably expect, and must have access to their accounts at all times.

88. Plaintiffs read Coinbase's representations that it was a "secure" platform and relied upon its representations in choosing to purchase and/or store cryptocurrencies and/or cash on Coinbase's platforms, as well as in choosing to link their Coinbase account to an account at another financial institution.

89. Coinbase is obligated by law to establish and maintain adequate cybersecurity measures.

90. Coinbase admits such measures should be "bank-level security standards:"

We deposit, transfer, and custody customer cash and crypto assets in multiple jurisdictions. In each instance, **we are required to safeguard customers' assets using bank-level security standards** applicable to

our wallet and storage systems, as well as our financial management systems related to such custodial functions.

Coinbase Global, Inc., Quarterly Report (Form 10-Q), at 83 (May 10, 2022) (emphasis added).

91. Coinbase recognizes the responsibilities, risks, and liabilities it undertakes holding its customers' valuable financial assets. For example, Coinbase made the following statement in its Supplement No. 1 to its April 1, 2021, prospectus filed with the Securities and Exchange Commission:

The Company has committed to securely store all crypto assets it holds on behalf of users. As such, the Company may be liable to its users for losses arising from theft or loss of user private keys. The Company has no reason to believe it will incur any expense associated with such potential liability because (i) it has no known or historical experience of claims to use as a basis of measurement, (ii) it accounts for and continually verifies the amount of crypto assets within its control, and (iii) it has established security around custodial private keys to minimize the risk of theft or loss. Since the risk of loss is remote, the Company had not recorded a liability at March 31, 2021 or December 31, 2020.

92. Coinbase also made the following statement in its Supplement No.1:

“Our Business involves the collection, storage, processing, and transmission of confidential information, customer, employee, service provider, and other personal data, as well as information required to access customer assets. We have built our reputation on the premise that our platform offers customers a secure way to purchase, store, and transact in crypto assets.”

## II. Cryptocurrency Held by Coinbase

93. When an owner of cryptocurrency transfers it, the unique addresses of the transferor and recipient are public, as well as the quantity of assets transferred.

94. Coinbase users may use the Coinbase platform both to hold and to exchange cryptocurrency.

95. When a Coinbase user entrusts cryptocurrency with Coinbase, Coinbase typically transfers that cryptocurrency from the deposit address where the user sent it to another address for storage.

96. Although Coinbase has often led users to believe otherwise, Coinbase, not the user, holds the “key” to cryptocurrency placed in a Coinbase account. On May 10, 2022, in a quarterly report filed with the Securities and Exchange Commission, Coinbase disclosed:

[I]n the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors. This may result in customers finding our custodial services more risky and less attractive and any failure to increase our customer base, discontinuation or reduction in use of our platform and products by existing customers as a result could adversely impact our business, operating results, and financial condition.

Coinbase Global, Inc., Quarterly Report (Form 10-Q), at 83 (May 10, 2022).

97. Trades on Coinbase’s exchanges do not happen directly between users but between a user and Coinbase. There is no privity between buyers and sellers on

Coinbase. The exchanges Coinbase operates are what are known as “centralized exchanges.” Centralized cryptocurrency exchanges act as an intermediary between a buyer and a seller and make money through commissions and transaction fees. These exchanges are created and run by a single company and are considered centralized because the one company oversees all the transactions and sets the exchange's rules and fees.

98. For example, in a cryptocurrency trade between Coinbase users, Coinbase debits the seller’s account and then credits the buyer’s account. The cryptocurrency is not transferred on the public digital ledger (or blockchain) for cryptocurrency. Rather, the only actual transactions are between the seller and Coinbase, on the one hand, and the buyer and Coinbase, on the other hand. Coinbase adjusts the “primary balance” of each user’s account.

99. When a user withdraws or transfers his or her cryptocurrency outside of Coinbase, the user provides Coinbase with the destination address for the cryptocurrency. Next, the exchange debits the user’s account and transfers a corresponding amount of cryptocurrency from Coinbase’s centralized reserves to that address. In other words, the withdrawn assets come from the centralized exchange. Coinbase often batches these transactions to reduce costs and so that Coinbase can profit from the transactions.

100. When Coinbase claims that a user owes it money or Coinbase deems a user's account to have a negative balance, Coinbase seizes the user's cryptocurrency, threatens to seize the user's cryptocurrency or funds, and/or indefinitely holds a user's *entire* account hostage – regardless of whether Coinbase's own valuation of the account exceeds what Coinbase alleges is owed and regardless of whether such amounts are the obligation of the user.<sup>2</sup> For example, if Coinbase claims a user owes it \$1,000, then Coinbase will promptly freeze an entire account with holdings Coinbase values at over \$5,000.

101. Additionally, a Coinbase user's account transaction history sometimes is altered, and users have a record of transactions that later are not included in their transaction history from Coinbase.

### **III. Coinbase Misleads Customers About Its Account Security**

102. Coinbase holds itself out as providing the primary financial account for the crypto economy – a safe, trusted, and easy-to-use platform to invest, store, spend, earn, and use cryptocurrency. For example, Coinbase's website states that it is the “most trusted” and “most secure” cryptocurrency platform and that assets held

---

<sup>2</sup> Coinbase seized, for example, Plaintiff Eric Larson's ETH2 and froze Plaintiff Wayne Colt Carter's entire account. *See also* Verified Answer by Defendant Coinbase, Inc., Gwinnett County Magistrate Court Case No. 20-M-01993 (Feb. 17, 2022).



online are protected by an “extensive insurance policy.”<sup>3</sup> Coinbase represents that it offers users the opportunity to participate in “a more fair, accessible, efficient, and transparent financial system enabled by crypto.”<sup>4</sup>

103. Coinbase’s home page states the company is “committed [to] “accessible, safe, and secure financial tools for everyone.”

104. The page at [www.coinbase.com/security](https://www.coinbase.com/security) has recently assured consumers of its “SECURITY FOR YOUR PEACE OF MIND,” prominently stating:

**98% of customer funds are stored offline**

Offline storage provides an important security measure against theft or loss.  
We distribute bitcoin geographically in safe deposit boxes  
and vaults around the world.

105. In January 2022, for example, Coinbase’s security webpage ([www.coinbase.com/security](https://www.coinbase.com/security)) assures consumers that it follows “Payment Industry Best Practices,” takes “careful measures to ensure your bitcoin is as safe as possible,” and that “Online Funds Are Now Covered by Insurance.” Coinbase’s annual report for 2021, Coinbase reveals that, even if its insurance coverage were to ever apply to a consumer’s loss, it is underinsured: the “total value of crypto assets in our

---

<sup>3</sup> <https://www.coinbase.com/security>.

<sup>4</sup> <https://www.coinbase.com/about>.

possession and control is significantly greater than the total value of insurance coverage that would compensate us in the event of theft or other loss of funds...”

106. Notwithstanding telling its shareholders that it was significantly underinsured, around July 2022, Coinbase’s security webpage touted Coinbase’s insurance coverage to customers:

Thanks to our best-in-class security practices, we’re the only crypto exchange to have never been hacked. We strategically store over 98% of deposits offline in secure cold storage facilities that are guarded and monitored 24/7. We also maintain an extensive insurance policy to protect assets held online.

107. Despite claiming it had “never been hacked,” Coinbase itself has admitted its “SMS Account Recovery process” was defective at least in 2021 and is well-aware it of its users losing funds in unauthorized transactions in recent years.

108. Coinbase represents to customers that it is a fully compliant, regulated entity, registered as a Money Services Business with FinCEN, the United States Department of the Treasury’s Financial Crimes Enforcement Network.

109. Coinbase also represents to consumers that it is licensed by the Georgia Department of Banking and Finance as a seller of payment instruments, along with holding similar money transmitter licenses in other states.

110. In providing “reasons why customers trust Coinbase,” Coinbase claims: “Coinbase has several security and financial certifications including Custody SOC 1,

Custody SOC 2, Prime Brokerage SOC 1, Prime Brokerage SOC 2, Cloud SOC 2, FINRA Broker Deal and FFIEC.”

111. On the Apple Mobile App store and the Google Play Mobile App store, Coinbase describes the Coinbase App as follows:

Coinbase: the simple, safe way to buy, store, trade and sell your crypto. The leading cryptocurrency exchange...

...

We're the world's most trusted cryptocurrency exchange, with over 103 million users across 100+ countries worldwide. Coinbase allows you to securely buy, hold and sell cryptocurrencies...

...

#### SECURE CRYPTOCURRENCY EXCHANGE

-Over 98% of cryptocurrency is stored securely offline and the rest is protected by industry-leading online security.

-Crypto accounts are subject to the same scrupulous safety standards, including multi-stage verification and bank-level security.

- Add a passcode to your crypto profile or remotely disable your phone's access to the app if it gets lost or stolen.

- Blockchains enable crypto to be bought and sent across the planet quickly and securely.

- Transfer crypto: Safe and secure asset movement to crypto wallets outside of the app.

...

112. On the Apple Mobile App store and the Google Play Mobile App store, Coinbase describes its “Coinbase Wallet” app to consumers as follows:

The all-new Coinbase Wallet mobile app is the easiest and safest way to buy NFTs, earn yield on crypto with staking or decentralized finance (DeFi), and access thousands of decentralized applications (dapps).

...

Wallet also makes it easy for you to securely store, send and receive ... hundreds of thousands of [digital assets] . . . Store digital assets in a secure, private wallet. You remain in control of your private keys, which are stored on your device using Secure Element technology. Because Coinbase Wallet is a self-custody crypto wallet, Coinbase never has access to your funds. You are in total control.

...

Industry-leading security

- Coinbase Wallet keeps your crypto and data safe so you can explore the decentralized web with confidence
- You remain in control of your private keys, which are stored only on your device using Secure Element technology
- Support for cloud backups of your recovery phrase help you avoid losing your assets if you lose your device or misplace your recovery phrase

113. In November 2021, Coinbase bragged to investors about providing the “highest level of security to protect [user] crypto assets” and having deployed “phishing-resistant security against bad actors.” Coinbase Global Inc., Quarterly Report at 47 (Form 10-Q) (Nov. 10, 2021).

#### **IV. The Truth About Coinbase’s Security in Practice**

114. Coinbase’s representations about its purportedly superior and bank-level security have proven untrue for both the Coinbase and Coinbase Pro exchange platforms and for the Coinbase Wallet.

115. Coinbase used false promises and deceptive statements to induce Plaintiffs and Class Members to trust Coinbase and to make them believe their accounts were secure with Coinbase, protected by Coinbase's purportedly rigorous security measures, and even insured against losses.

116. Coinbase systematically fails to implement adequate and standard security measures to prevent fraudulent account access, to detect fraudulent activity, and to remediate the fraudulent activity. As shown by Plaintiffs' experiences, Coinbase ignores obvious red flags signaling to Coinbase suspicious activity and a risk of theft.

117. Even when users request Coinbase to secure their account or reverse an unauthorized transfer of cash, Coinbase fails to promptly secure the account and reverse the transactions, leaving users helpless to watch their accounts drained. While it refuses to reverse or help retrieve funds withdrawn from user accounts without authorization, Coinbase is taking action to retrieve what it considers funds improperly withdrawn during an exchange rate glitch Coinbase blamed on a third-party technical issue.<sup>5</sup>

---

<sup>5</sup> See <https://www.coindesk.com/business/2022/10/17/coinbase-threatens-to-sue-crypto-traders-who-profited-from-pricing-glitch/>.

118. Coinbase’s woefully inadequate customer support is not only infuriating for customers but is ineffective and leaves users’ accounts at risk. Many users are unable to reach a Coinbase Support representative, and if they do, the representative cannot or does not assist them. The written responses from “Coinbase Support” are repeatedly inaccurate, non-responsive, stalling, superficial, incongruous, and appear to be automated responses. Multiple Plaintiffs even received emails from Coinbase addressing them by the wrong name. For Plaintiff Eric Larson, Coinbase repeatedly added the random email address of a “Linda” as an email recipient, even after Mr. Larson alerted Coinbase of its glaring mistake.

119. Coinbase does not have sufficient customer support representatives who speak Spanish, which has caused or exacerbated the harm to Spanish-speaking customers. The insufficient customer support in Spanish is despite Coinbase being an international company and despite Coinbase supposedly being “supported” in Spanish speaking countries.

120. Coinbase’s neglect for vital customer service processes appears to be a deliberate, calculated, and narrow-minded business strategy to pursue rapid user growth at all costs. In its quarterly report on August 9, 2022, Coinbase admitted to its investors the “increased operational risks” of its focus on profit over user account security:

**We rely on third parties** in connection with many aspects of our business, including . . . third parties **that provide outsourced customer service**, compliance support and product development functions, which are critical to our operations. Because we rely on third parties to provide these services and to facilitate certain of our business activities, we face increased operational risks. We do not directly manage the operation of any of these third parties, including their data center facilities that we use. **These third parties may be subject to** financial, legal, regulatory, and labor issues, **cybersecurity incidents**, break-ins, computer viruses, denial-of-service attacks, sabotage, acts of vandalism, **privacy breaches**, service terminations, disruptions, interruptions, and other misconduct. (Emphasis supplied).

121. Like a bank vault left wide open with a neon sign over the door that says “Take Me,” Coinbase’s exchange and Wallet platforms are so riddled with security flaws that Coinbase left Plaintiffs and Class Members’ funds vulnerable to be carried off by hackers and third-party bad actors. Had Coinbase bothered to put in place adequate cybersecurity protections, unauthorized access, unauthorized conversions of cryptocurrency, unauthorized transfers of funds from user bank accounts, and the freezing of user accounts would not have occurred or could have been appropriately remediated.

122. In its 10-K annual report for 2021, Coinbase admitted it had flawed data security measures and that it is a target for hackers:

[I]n 2021, third parties independently obtained login credentials and personal information for at least 6,000 customers and used those credentials to exploit a vulnerability that previously existed in the account recovery process. Coinbase reimbursed impacted customers approximately \$25.1 million.

Coinbase Global, Inc., Annual Report at 63 (Form 10-K) (Feb. 25, 2022).<sup>6</sup>

123. That data breach occurred in March 2021, but Coinbase did not report it until September 27, 2021.<sup>7</sup>

124. Coinbase has also admitted the “Coinbase Wallet” has major security vulnerabilities and can be drained even if a user’s “recovery phrase” is never revealed. Like Coinbase exchange accounts, the Coinbase Wallet lacks the ability to detect numerous “red flags” indicative of fraud, leaving users to helplessly watch their savings drained without warning and without their authorization.

125. For example, the Coinbase Wallet allows some “smart contracts” to drain a user’s Coinbase Wallet Account of cryptocurrency without the user receiving a warning of the withdrawal.

126. In response to questions about scammers and bad actors taking advantage of Coinbase users, Coinbase’s Chief Security Officer, Philip Martin, acknowledged that “some bad actors are going to get on [Coinbase].” When pressed on Coinbase’s security flaws that leave users accounts vulnerable to financial ruin,

---

<sup>6</sup> An earlier section in the same annual report touted a “heritage of security,” claiming: “We are proud to be one of the longest-running crypto platforms where customers have not lost funds due to a security breach of the platform and we secure our customers’ funds with multiple layers of protection by employing what we believe to be the largest hot wallet security program in the insurance market.” Annual Report at 8.

<sup>7</sup> See <https://oag.ca.gov/system/files/09-24-2021%20Customer%20Notification.pdf>



he acknowledged: “I’m not going to sit here and say Coinbase Wallet has the perfect [user interface]. Are there improvements we could make? Absolutely. And we will continue to do so.”<sup>8</sup>

127. The Coinbase Wallet does not warn users of its vulnerabilities and the risks of “smart contracts” that can drain a Coinbase Wallet without authorization from the user.

128. As disclosed in its privacy policy, Coinbase collects detailed personal data on its users.<sup>9</sup> As Plaintiffs’ experiences show, Coinbase uses the detailed personal data it collects to enrich itself, yet Coinbase does not use that data for the benefit of users to detect and prevent unauthorized activity in their accounts.

129. The Apple App Store discloses that the Coinbase Exchange App collects a plethora of personal data about users, including the following data linked to users’ identity:

- Purchases (Purchase History)
- Financial Info (Payment Info, Credit Info, Other Financial Info)
- Contact Info (Physical Address, Email Address, Name, Phone Number)
- Identifiers (Device ID)
- Usage Data (Product Interaction)
- Sensitive Info

---

<sup>8</sup> See <https://www.washingtonpost.com/technology/2022/04/04/crypto-scams-coinbase-liquidity-mining/>.

<sup>9</sup> <https://www.coinbase.com/legal/privacy>.

- Diagnostics (Crash Data, Performance Data, and Other Diagnostic Data)
- Other Data

130. In violation of its representations to users, Coinbase ignores red flags signaling suspicious activity and approves account activity that is completely inconsistent with users' previous activity on their Coinbase accounts. Despite red flags, Coinbase failed to delay the processing or execution of withdrawals that emptied Plaintiffs' accounts.

131. For example, in violation of its representations to users, Coinbase does not take action on red flags such as:

- emptying an account from a new device with an IP address indicating a location far away from the user's current and usual location;
- changing an account's email addresses to a disposable account with a YOPmail domain (which are not password protected email accounts);
- a password change alongside the emptying of an account;
- changing the phone number on an account;
- changing the name on an account;
- complete withdrawals requested after a Coinbase account has been frozen or a user has reported unauthorized activity;
- withdrawing all of an account's funds to a new account that is not in the user's name; and/or
- immediately withdrawing the entire account's balance to a newly added account or destination previously unaffiliated with the user.

132. Coinbase's approval of the immediate depletion of accounts without authorization or warning is inconsistent with industry standards.

133. While user accounts are being looted, Coinbase collects fees from unauthorized transactions.

134. Coinbase holds a BitLicense from the New York Department of Financial Services (“NYDFS”) and is therefore subject to examinations and investigations by the NYDFS. Upon information and belief, NYDFS is currently investigating Coinbase’s compliance program (including compliance with the Bank Secrecy Act and sanctions laws), cybersecurity, and customer support.

135. On August 30, 2022, the House Committee on Oversight and Reform sent a letter and request for document to Coinbase, requesting information about what Coinbase is doing to combat cryptocurrency-related fraud. The letter observed:

Insufficient security measures likewise leave users exposed to the outright theft of assets stored on the exchange. Many exchanges have also failed to implement appropriate monitoring of accounts, which can flag illicit activity, notify investors, and prevent transactions with addresses linked to scammers.

**V. Coinbase’s “User Agreement” and Sham Dispute Resolution Process**

136. Coinbase has claimed to bind its users, such as Plaintiffs and Class Members, to a lengthy “User Agreement” when they create their account with Coinbase.

137. Coinbase cannot shirk its duties to users through disclaimer language buried on its website or buried in a purported “User Agreement,” which is constantly being revised and in flux.

138. From 2017 until the present, the User Agreement has been revised at least approximately fifty times – including at least thirteen times in the last year. Indeed, Coinbase has revised the User Agreement since this action was filed. The “last updated” date on the face of the User Agreement, Coinbase has admitted, does not even get changed with every revision of the User Agreement.

139. A recent iteration of the User Agreement is over 50 pages long single-spaced, excluding terms purportedly incorporated by reference and other terms that may apply to a user’s relationship with Coinbase.

140. Coinbase’s website also presents a “Cardholder Agreement.”<sup>10</sup>

141. Coinbase’s website also presents the Coinbase Wallet Terms of Service Agreement.<sup>11</sup>

142. Although the User Agreement purports to include an arbitration provision, the provision is unconscionable, one-sided, and contains a number of cumbersome conditions precedent that must be met before Coinbase users can

---

<sup>10</sup> See <https://www.coinbase.com/legal/coinbasecard>.

<sup>11</sup> See <https://wallet.coinbase.com/terms-of-service>.

arbitrate their disputes with Coinbase. As described below, it is nearly impossible to make any sense of those long and chaotic conditions.

143. First, Coinbase requires customers to use its “support team,” a condition inapplicable to Coinbase. If the user and Coinbase fail to resolve the user’s dispute in that manner, then users must utilize Coinbase’s “Formal Complaint Process,” another condition not applicable to Coinbase.

144. The Formal Complaint Process involves submitting *another* complaint to “Coinbase Customer Support,” apparently distinct from “Coinbase Support,” using Coinbase’s “complaint form.”

145. Coinbase Support, whether on the phone or in writing, very often did not (and, upon information and belief, may still not) direct users to the so-called “Formal Complaint Process.” When a Coinbase Support ticket is unresolved and inappropriately “closed” by Coinbase, Coinbase often does not even mention a “Formal Complaint.”

146. When Coinbase Support’s response does briefly mention a “Formal Complaint,” the responses often do not direct users to the “Formal Complaint” form on its website. Rather, Coinbase sends users to a Coinbase webpage where Coinbase users may submit another complaint to Coinbase Support, resulting in a frustrating vicious cycle for users. From the link provided to users for the “Formal Complaint,”

users would have to navigate the labyrinth of Coinbase’s website to find the actual “Formal Complaint” form.

147. The various Coinbase User Agreements direct written “formal” complaints to an online form and an address in Manhattan’s financial district: 82 Nassau St #61234, New York, NY 10038. This is not the address of any office providing customer support, much less a Coinbase office. As shown below, it is the address of a UPS Store that offers “a mailbox with a real street address.”



*The UPS Store*, available at <https://goo.gl/maps/Uk32PY2PmF7cNRdj7>.

148. Confusingly, the Dispute Resolution section of the current User Agreement separately directs Plaintiffs still further addresses, stating: “Coinbase requires that all legal documents . . . be served on our registered agent for service of process.”

149. The Coinbase Help page for how to submit a complaint provides a *different* UPS Store box number than the User Agreement page. It directs users to send a “written complaint” to 82 Nassau St. #60178 New York, NY 10038. <https://help.coinbase.com/en/coinbase/other-topics/other/how-to-send-a-complaint>

150. Coinbase Support emails do not provide (either) address of the above Manhattan UPS Store for Formal Complaints.

151. The “Formal Complaint” link in the User Agreement now on Coinbase’s website does not directly link to the online complaint form customers must use, despite what the User Agreement states. Instead, it links to a Coinbase Help page<sup>12</sup> that spans over a page, single-spaced; that page ultimately discourages users from submitting a “Formal Complaint.” Buried in the middle of that page, is a link to a “complaints form.”

---

<sup>12</sup> <https://help.coinbase.com/en/coinbase/other-topics/other/how-to-send-a-complaint>

152. Even worse, older versions of Coinbase’s User Agreement linked to the general Coinbase Help page, explaining only that the complaint form can be found among the “Coinbase support pages” or “can be requested from Coinbase Customer Support.”

153. Apparently, the online Formal Complaint form can be found at <https://help.coinbase.com/en/contact-us/submit-a-complaint>. As shown below, nowhere on that webpage (or even in the url) does it say that the form is the “Formal Complaint” form.



## Submit a complaint

**1** Please fill in the required fields below. Once you have submitted your complaint, our Customer Complaint Officer will review and respond within 15 business days. You can read more about our complaints process and next steps in our [User Agreement](#) or [Support Center](#).

First Name \*

Please add your first name

Surname \*

Your Last Name

Phone Number \*

Best number to contact you

Country \*

Select a country

Email Address (Associated with your Coinbase account) \*

Email Address

Product \*

Select an option

What does your complaint relate to? \*

Select an option

Please describe your complaint: \*

Please describe the incident and complaint in full detail and describe how we can address it to your satisfaction.

To protect your privacy, please ensure you are not providing any personal identifying information when submitting this request.

Does your complaint relate to a support case? \*

Yes

No

Have you filed a formal complaint with Coinbase about this issue before? \*

Yes

No

Does your complaint involve a monetary claim? \*

Yes

No

Submit

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

154. The current online Formal Complaint form warns users they “must first submit a ticket through Coinbase Support before filing a complaint” and enter the user’s 8 digit “support case number.”

155. The online Formal Complaint form further warns users not to submit a Formal Complaint unless they “allow 5-7 business days for [Coinbase’s] Support Team to assist.” The form requires users to input an 8-digit support case number.

Does your complaint relate to a support case? \*

Please enter your 8 digit support case number (Please include leading zeros) \*

Example Case Number: 01234567

Has the issue been resolved by our Support Team? \*

**i** Please allow 5-7 business days for our Support Team to assist you.

156. The online Formal Complaint form asks users if they have “filed a formal complaint with Coinbase about this issue before?” If a user selects yes, the user is required to enter the “complaint case number,” which is 8-digits like the

“support case number.” The “complaint case number” is, upon information and belief, actually the same as a “support case number” if one already has been assigned.

Have you filed a formal complaint with Coinbase about this issue before?\*

Please enter your 8 digit complaint case number (Please include leading zeros)\* (i)

Example Case Number: 01234567

157. The online form also contains a bizarre and distressing warning, especially considering the experiences of Plaintiffs:

**To protect your privacy, please ensure you are not providing any personal identifying information when submitting this request.**

158. After submitting a Formal Complaint using Coinbase’s online form, Coinbase does not send users a copy of the submitted form.

159. On or about January 21, 2022, the screen after Mr. Onimus submitted a complaint using Coinbase’s online form stated, in part, that Coinbase is “currently receiving a high number of requests so we may take longer to respond...” And it continued by discouraging further complaints with Coinbase or others, adding:

“Please also **do not contact our partner banks**, as they will be unable to assist you since your account is managed by Coinbase.”

160. According to the User Agreement, it can take up to 45 business days to receive a response to a Formal Complaint. In other words, after managing to submit a formal complaint, a user still has to wait over two months since the already long waiting period excludes weekends and holidays.

161. Coinbase has attempted to unilaterally extend this waiting period.

162. On the Coinbase Help page for how to submit a complaint (which the User Agreement links to), Coinbase further attempts to unilaterally extend the waiting period after submitting a Formal Complaint, stating “**Please allow an additional 10 days for processing when using postal mail submissions.**”

163. In total, Coinbase asks users to wait *over three months* before filing a claim: 7 business days for Coinbase Support to take action, plus 45 business days for the Formal Complaint process, and plus an additional 10 days for a mailed Formal Complaint.

164. If the Formal Complaint is submitted using the form on Coinbase’s website, the user does not receive a copy of the Formal Complaint. The user receives an email confirming receipt of the complaint and stating the “internal complaints process will need to be completed before any litigation is initiated.”

165. If the lengthy Formal Complaint Process fails to resolve the customer's dispute, only then can customers attempt to resolve disputes through arbitration. However, Coinbase systemically fails to follow its own pre-arbitration dispute resolution mechanisms as set forth in the User Agreement, thereby rendering the provision, including its delegation provision, void as to Plaintiffs and Class Members.

166. Moreover, for claims against users, Coinbase does not subject itself to the purported dispute process, arbitration clause in the User Agreement, or the delegation clause therein.

167. Coinbase knew, or should have known, that when presenting Plaintiffs and Class Members with its User Agreement, Coinbase did not have adequate staffing or adequate policies, practices and procedures in place to follow its mandated pre-arbitration dispute resolution procedures incorporated into, and a prerequisite for, the Arbitration provision in the User Agreement. Indeed, Coinbase has even disclosed that its "phone agents" do not take support calls for many types of customer inquiries.

168. Coinbase forced users into entering an unconscionable User Agreement knowing that Coinbase would breach the requirements of the User Agreement's dispute resolution process. The arbitration clause, delegation clause, and long pre-

arbitration dispute resolution processes serve no legitimate business purpose. The length of the pre-arbitration dispute resolution process leaves users in limbo for months while they are unable to trade, buy, or sell cryptocurrency and/or after having lost significant assets due to Coinbase's negligence.

169. Accordingly, Coinbase misrepresented its ability to comply with its own arbitration procedures and fraudulently induced Plaintiffs and Class Members to accept the dispute resolution clause, including the provision delegating arbitrability and the contract's validity to the arbitrator.

170. The User Agreement's dispute resolution process is procedurally unconscionable. Moreover, the procedural unconscionability of the User Agreement is expressly incorporated in the User Agreement's unusual "delegation clause" that "decides who decides" disputes. The delegation clause imposes an onerous, unfair, and unusual burden on users because the delegation clause itself is subject to the multi-step, onerous dispute resolution process in the User Agreement.

171. Further, the cumbersome and onerous dispute resolution process in Coinbase's User Agreement (including the delegation clause specifically) is one-sided. The long, multi-step process of contacting Coinbase's "support team" and using the "Formal Complaint Process" only applies to claims users seek to make against Coinbase. Coinbase is not subject to those obstacles.

172. Because Coinbase is immune from the pre-arbitration hoops it set in front of users, the User Agreement does not require Coinbase to arbitrate its claims against users.

173. At the request of the American Arbitration Association (“AAA”), on February 3, 2022, Coinbase agreed to waive the following provision in a version of the User Agreement’s arbitration clause:

Disputes involving claims, counterclaims, or requests for relief under \$25,000, not inclusive of attorneys’ fees and interest, will be conducted solely on the basis of documents you and Coinbase, submit to the arbitrator.

174. According to the AAA, the above provision has a material or substantial deviation from the AAA Consumer Arbitration Rules and/or the AAA’s standards for due process.

175. Nonetheless, Coinbase continues to include it the many subsequent versions of the prolix User Agreement on the Coinbase website.

176. Plaintiffs read Coinbase’s representations about its products and services, including about the high security of Coinbase’s platforms and Coinbase’s Support resources, and relied on those representations in purchasing and storing assets with Coinbase.

**IV. Coinbase's Failure to Implement Account Protections Causes Plaintiffs to Lose Access to Their Accounts and Funds**

**A. Coinbase Fails to Protect Accounts and Fails to Ensure Reliable Access to Cryptocurrency in Accounts**

**Ms. Adams's Coinbase Account**

177. Ms. Adams held cryptocurrency in her Coinbase account.

178. On or about April 25, 2022, without Ms. Adams's authorization or knowledge, Coinbase approved the conversion of Ms. Adams's cryptocurrency to Bitcoin, and then then transfer of the over \$1,000 worth of Bitcoin to a Coinbase Pro account unassociated with Ms. Adams.

179. Ms. Adams never received notice of the above transactions, and only became aware of the above-referenced unauthorized transactions when she checked her Coinbase account around early September.

180. Ms. Adams notified Coinbase of the unauthorized transactions.

181. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Adams has been damaged by the loss of cryptocurrency from her Coinbase account.

**Mr. Alexander's Coinbase Account**

182. Mr. Alexander held cryptocurrency in his Coinbase account.



183. On or about June 18, 2022, without Mr. Alexander's authorization or knowledge, Coinbase approved the sale of Mr. Alexander's cryptocurrency, converting them into approximately \$3,504.81 in cash, which was then drained from his account.

184. Mr. Alexander discovered the above withdrawals from his Coinbase account when he logged into the Coinbase app. He notified Coinbase of the unauthorized transactions.

185. On or about October 2, 2022, Mr. Alexander received notice of a withdrawal of \$23.88 from his Coinbase account. Mr. Alexander did not authorize that withdrawal.

186. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Alexander has been damaged by the loss of cryptocurrency and funds from his Coinbase account.

#### **Mr. Axelsson's Coinbase Account**

187. Mr. Axelsson began holding cryptocurrency in his Coinbase account in 2020.

188. After being unable to login to his account, Mr. Axelsson learned his Coinbase account was compromised on or about November 26, 2021.

189. Coinbase allowed transactions converting the cryptocurrencies in Mr. Axelsson's Account to Stellar Lumens (XLM). Mr. Axelsson's entire account balance was drained, causing him to lose cryptocurrency worth more than about \$60,000 at the time.

190. In addition, Coinbase allowed requests for \$70,000 in additional funds from Mr. Axelsson's account with another financial institution.

191. Mr. Axelsson's bank did not fulfill all of those unauthorized requests, and the bank reversed a transfer from Mr. Axelsson's account.

192. Thereafter, Coinbase claimed Mr. Axelsson owed it \$36,625.55, which needed to be paid before he would be eligible to make purchases again on Coinbase.

193. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Axelsson has been damaged by the loss of cryptocurrency he entrusted with Coinbase.

#### **Ms. Bennett's Coinbase Account**

194. Ms. Bennett held cryptocurrency in her Coinbase account.

195. Coinbase allowed a new device, with an IP address associated with Denmark, to access Ms. Bennett's Coinbase account.

196. Coinbase also allowed an unknown person to change the email on Ms. Bennett's Coinbase account to an email address at the domain

“@YOPmail.com.” YOPmail offers temporary disposable email addresses that are not password protected.

197. On or about February 17, 2022, without Ms. Bennett’s approval (or knowledge), Coinbase approved the conversion of Ms. Bennett’s cryptocurrency holdings and a withdrawal of approximately \$14,318.48 in cryptocurrency from Ms. Bennett’s account to a new external location.

198. On or about February 17, 2022, Ms. Bennett notified Coinbase of these unauthorized transactions.

199. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Ms. Bennett has been damaged by the loss of cryptocurrency she entrusted with Coinbase.

### **Mr. Bigonia’s Coinbase Account**

200. Mr. Bigonia held cryptocurrency in a Coinbase account.

201. On or about July 9, 2022, thousands of dollars of cryptocurrency were withdrawn from Mr. Bigonia’s account without his authorization.

202. Mr. Bigonia informed Coinbase of the unauthorized transactions in his account.

203. Since then, Coinbase has repeatedly restricted and prevented Mr. Bigonia from accessing his account or from purchasing cryptocurrency.

204. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Bigonia has been damaged by the loss of cryptocurrency entrusted with Coinbase and the loss of consistent control over the cryptocurrency in his Coinbase account.

#### **Mr. Blumetti's Coinbase Account**

205. Mr. Blumetti opened an account with Coinbase around 2015 or 2016 and held cryptocurrencies in his Coinbase account.

206. On April 7, 2021, Mr. Blumetti had previously asked for assistance from Coinbase Support regarding an account issue. Mr. Blumetti received a call that appeared to be from Coinbase Support. After Mr. Blumetti spoke with the purported Coinbase representative, Coinbase approved requests to convert Mr. Blumetti's cryptocurrency into Bitcoin and withdraw all of the cryptocurrency from Mr. Blumetti's Coinbase account to external locations.

207. Mr. Blumetti never authorized the conversion of his cryptocurrency into Bitcoin, and he never authorized the withdrawal of cryptocurrency from his Coinbase account.

208. On April 7, 2021, Mr. Blumetti immediately contacted the Coinbase Support to secure his account. Mr. Blumetti was not able to reach a support

representative at that telephone number, so he was forced to attempt to secure his Coinbase account using the slow automated telephone support system.

209. Coinbase locked Mr. Blumetti out of his account for over one month after the hack occurred. During that time, Mr. Blumetti only received generic, confusing, and automated emails from Coinbase that did not respond to his communications.

210. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Blumetti has been damaged by the loss of cryptocurrency worth approximately over \$670,829.23 entrusted with Coinbase.

### **Mr. Bradley's Coinbase Account**

211. Mr. Bradley opened a Coinbase account in November 2021 where he held over \$2,000 worth of cryptocurrencies.

212. In April 2022, Mr. Bradley discovered he was unable to login to his account.

213. In April 2022, Mr. Bradley received a password reset email from Coinbase that was addressed to "Alexander Ross," which, of course, is not Mr. Bradley's name or a name on his account. When Mr. Bradley contacted

Coinbase and requested access to his account, the email from Coinbase Support to Mr. Bradley was addressed “Hello Alexander, . . .”

214. Mr. Bradley never consented to a change in the name on his Coinbase account. He never received a two-factor authentication code for any such change.

215. As a result of Coinbase’s conduct, Mr. Bradley has been unable to access his cryptocurrency or account despite repeated requests to Coinbase for help and information about his cryptocurrency.

### **Mr. Bray’s Coinbase Accounts**

216. Mr. Bray had a Coinbase account and Coinbase Pro account. Mr. Bray held cryptocurrency in his Coinbase account.

217. On or about October 20, 2021, Mr. Bray discovered unauthorized transactions withdrawing his cryptocurrency from his account to an external location.

218. Mr. Bray promptly notified Coinbase of the unauthorized withdrawals of his cryptocurrency, which was then worth approximately \$172,061.45.

219. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Mr. Bray has been damaged by the loss of cryptocurrency entrusted with Coinbase in his account.

### **Mr. Calderón's Coinbase Account**

220. Mr. Calderón had a Coinbase Pro account in which he held cryptocurrency.

221. On or about September 19, 2022, Coinbase restricted access to Mr. Calderón's Coinbase Pro account. Coinbase claimed it transferred his cryptocurrency from his Coinbase Pro account to a (regular) Coinbase exchange account from which Coinbase instructed Mr. Calderón to withdraw his holdings.

222. While it appears some cryptocurrency was transferred, Mr. Calderón has lost access to over \$100,000 worth of Bitcoin that was held in his Coinbase Pro account.

223. Mr. Calderón submitted a "Formal Complaint" to Coinbase.

224. Coinbase has not explained the vanishing of Mr. Calderón's Bitcoin, and has refused to reverse or credit the unauthorized transactions in Mr. Calderón's account.

225. As a result of Coinbase's conduct, Mr. Calderón has been damaged by losing access to the cryptocurrency held in his account and losing substantial cryptocurrency holdings entrusted with Coinbase.

### **Mr. Colt Carter's Coinbase Account**

226. Mr. Colt Carter held cryptocurrency in his Coinbase account.

227. On or about October 11, 2022, Mr. Colt Carter attempted to transfer funds into his Coinbase account from an account at another financial institution.

228. In the days after the transfer, Mr. Colt Carter saw that the funds were debited from his account at the other financial institution, but Coinbase had failed to credit any transfer of funds in his Coinbase account. The other financial institution reversed the transfer to Mr. Colt Carter's Coinbase account.

229. Coinbase then claimed Mr. Colt Carter owed it \$1,000.

230. Further, Coinbase froze Mr. Colt Carter's entire Coinbase account, which includes cryptocurrency valued by Coinbase at more than \$1,000. Coinbase disabled his ability to make bank purchases/deposits, buy/sell digital currency, or send digital currency.

231. According to an automated message from Coinbase, unless Mr. Colt Carter pays Coinbase \$1,000 on October 21, 2022, Coinbase will "begin an automatic recovery" on October 22, 2022, which "could include selling [his] cryptocurrency holdings on both Coinbase and Coinbase Pro."

232. As a result of Coinbase's conduct, Mr. Colt Carter has been deprived of access to the cryptocurrency in his Coinbase account.



### **Mr. Chiulli's Coinbase Account**

233. Mr. Chiulli opened a Coinbase account in August 2017 and added a Coinbase Pro account in September 2021.

234. Beginning on November 13, 2021, Mr. Chiulli was locked-out of his Coinbase Pro account on several occasions, including for five consecutive days.

235. On November 17, 2021, in attempting to resolve the inability to access his Coinbase Pro account, Mr. Chiulli used a search engine to find a telephone number for Coinbase. At the top of the search results, there was a telephone number with an area code for San Francisco, California, where Coinbase has an office.

236. The person who answered the phone represented that he was a Coinbase Support representative and proceeded to assist Mr. Chiulli with regaining access to his Coinbase accounts and helping to reset his account password.

237. After Mr. Chiulli hung up the phone, he received an email alerting him of two transfers of cryptocurrency from his accounts to an external location, depleting his accounts of all Bitcoin in a manner completely inconsistent with his prior behavior on his Coinbase accounts.

238. Mr. Chiulli immediately realized his account had been compromised and used a search engine to find the telephone number for Coinbase Customer

Service. A toll-free number appeared at the top of the search for Coinbase Customer Service.

239. A person claiming to be a “senior Coinbase software engineer” answered the phone and offered to help Mr. Chiulli recover the Bitcoin stolen from his account. Upon realizing this person was an imposter and not associated with Coinbase, Mr. Chiulli stopped speaking with the fraudster.

240. That same day, Mr. Chiulli conducted another internet search for Coinbase’s Customer Service telephone number and found the correct telephone number. After being on hold for two hours, Mr. Chiulli informed Coinbase there were unauthorized transactions on his account. A Coinbase representative identified the withdrawals from his account and transferred his call to Coinbase’s Fraud Prevention Department. Coinbase’s Fraud Prevention Department promised to investigate and contact him in three to five days.

241. Mr. Chiulli also notified Coinbase Support in writing that same day of the unauthorized transactions in his accounts.

242. Mr. Chiulli has never heard back from Coinbase’s Fraud Prevention Department. Coinbase never provided a substantive response to Mr. Chiulli. Coinbase only sent Mr. Chiulli automated responses and requested that his support case be “closed.”

243. The “Account History” of Mr. Chiulli’s Coinbase and Coinbase Pro accounts no longer show the unauthorized, fraudulent transactions depleting his accounts. Coinbase has failed to display (or has deleted) the records of the fraudulent transactions from his account history.

244. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Mr. Chiulli lost over \$155,000 worth of cryptocurrency entrusted with Coinbase.

#### **Ms. Cohen’s Coinbase Account**

245. Ms. Cohen opened a Coinbase account in 2017.

246. In November 2021, Coinbase allowed an unknown third-party, to gain access to Ms. Cohen’s Coinbase account after numerous failed sign-in attempts from multiple IP addresses not located in Ms. Cohen’s area.

247. Coinbase then allowed an unknown person to link new bank account(s) to Ms. Cohen’s Coinbase account, allowed an attempt to withdraw funds from Ms. Cohen’s bank account, allowed the unauthorized conversion of cryptocurrencies into cash, and then allowed over \$25,000 in cash to be withdrawn from Ms. Cohen’s account into the newly added bank account(s).

248. Coinbase also allowed an unknown person to request funds from Ms. Cohen’s bank account and use them to purchase cryptocurrency. The newly

purchased cryptocurrency was then immediately converted back into cash and transferred to the newly added bank account(s).

249. Ms. Cohen promptly notified Coinbase of the unauthorized transactions in her account.

250. Coinbase demanded Ms. Cohen pay \$1,000 to regain full access to her Coinbase account.

251. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase conduct, Ms. Cohen has been damaged by the loss of cryptocurrencies and cash held in her Coinbase account.

#### **Mr. Eliezaire's Coinbase Account**

252. Mr. Eliezaire created a Coinbase account on or about January 20, 2021.

253. On October 24, 2021, an unknown person changed the email address and phone number for Mr. Eliezaire's Coinbase account holding cryptocurrency. Coinbase allowed that person to request \$1,000 from Mr. Eliezaire's connected bank account and then purchase cryptocurrency. According to Coinbase, Coinbase then allowed the unknown person to convert Mr. Eliezaire's cryptocurrencies into Bitcoin and then withdraw nearly all Bitcoin out of Mr. Eliezaire's Coinbase account to an external location.

254. On or about October 25, 2021, Mr. Eliezaire contacted Coinbase by telephone and then by email notifying Coinbase that his account had been compromised.

255. Mr. Eliezaire informed Coinbase that the transfers on October 24, 2021, including the nearly complete depletion of his account and transfer from his bank account, were unauthorized.

256. Coinbase never restored access to Mr. Eliezaire's original Coinbase account. Coinbase instead transferred approximately \$3.20 worth of Bitcoin from Mr. Eliezaire's original Coinbase account to a new Coinbase account for Mr. Eliezaire to use.

257. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Eliezaire has been damaged by the loss of his cryptocurrency entrusted with Coinbase.

### **Mr. Garcia's Coinbase Account**

258. Mr. Garcia had a Coinbase account holding cryptocurrency.

259. On September 10, 2022, Mr. Garcia received an email indicating suspicious activity in his Coinbase account.

260. Mr. Garcia promptly contacted Coinbase, requested Coinbase secure his account, and informed Coinbase that any withdrawals from his account were

unauthorized. A Coinbase representative named Bhagya responded that Mr. Garcia's Coinbase account would be locked until his identity could be verified. Mr. Garcia completed the Coinbase identity verification process in the Coinbase application.

261. In the same conversation, Mr. Garcia was also told that his account showed a withdrawal of \$11,682.43. Coinbase urged Mr. Garcia to wait until he regained access to his account to learn more.

262. On September 15, 2022, Mr. Garcia's account was finally unlocked. Upon entering his account for the first time in five days, Mr. Garcia found his funds completely drained.

263. Mr. Garcia did not authorize the withdrawal, and Coinbase would not provide any further information regarding the unauthorized transaction.

264. Again, Mr. Garcia contacted Coinbase, spoke to a representative, and requested information about the unauthorized transaction. The Coinbase representative informed Mr. Garcia that they did not have such information. Mr. Garcia requested an escalation of his case but did not receive assistance.

265. On September 19, 2022, Mr. Garcia received an email from Coinbase stating that they were closing his case.

266. Again, Mr. Garcia contacted Coinbase to no avail, and, again, the Coinbase representative could not provide Mr. Garcia with any information regarding the unauthorized withdrawal from his Coinbase account.

267. On October 4, 2022, Coinbase finally emailed Mr. Garcia to tell him \$11,682.43 was withdrawn from his account on September 10, 2022 at 6:29 p.m. P.D.T. The email added: “Coinbase is unable to reverse transactions.”

268. Mr. Garcia has submitted a Formal Complaint with Coinbase.

269. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Mr. Garcia has been damaged by the loss of access to his account and the loss of his cryptocurrency holdings entrusted with Coinbase.

### **Mr. Girshovich’s Coinbase Account**

270. Mr. Girshovich held cryptocurrency in his Coinbase account in which he held cryptocurrency.

271. On November 8, 2021, Coinbase allowed a third-party actor to convert the cryptocurrency in his Coinbase account into cash and then withdraw approximately \$14,482.08 from his account into a newly added checking account at a bank located across the country from Mr. Girshovich.

272. On November 9, 2021, Mr. Girshovich notified Coinbase that the above transactions, including the emptying of his account, were not authorized by him and he had no connection with the newly added bank account.

273. Coinbase refused to stop or reverse the transfer from his account.

274. The access history for Mr. Girshovich's Coinbase's account does not show a login from any device on November 8, 2021.

275. In response to Mr. Girshovich's communications, Coinbase sends automated emails and refuses to provide information.

276. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Girshovich has been damaged by the loss of his cryptocurrency holdings entrusted with Coinbase and the loss of funds from his Coinbase account.

### **Mr. Glackin's Coinbase Account**

277. Mr. Glackin held cryptocurrency in his Coinbase account.

278. Mr. Glackin secured his Coinbase account with two-factor authentication sent to a device secured by facial recognition.

279. On or about January 20, 2020, Mr. Glackin logged-in to his Coinbase account and discovered nearly all of his cryptocurrency had vanished.



280. According to Coinbase, on or about January 8, 2020, cryptocurrency was transferred from Mr. Glackin's Coinbase account to a Coinbase Pro account. Mr. Glackin did not have a Coinbase Pro account. Then, in a series of transactions, the cryptocurrency was drained from the Coinbase Pro account.

281. Mr. Glackin never received notice or gave authorization for any of these transfers.

282. In fact, Mr. Glackin, himself, notified Coinbase of the unauthorized transactions, to which Coinbase responded by locking him out of his account and refusing to provide any information about the loss.

283. Since regaining access to his Coinbase account, Mr. Glackin has repeatedly lost access to his account, including one instance for a period of seven months.

284. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Glackin has been damaged by the loss of his cryptocurrency entrusted with Coinbase.

### **Mr. Hastings' Coinbase Account**

285. Mr. Hastings held cryptocurrency in his Coinbase account.

286. On or about March 15, 2022, a third party gained access to Mr. Hastings' Coinbase account, converted Mr. Hastings' cryptocurrency, and then

transferred the converted cryptocurrency from Mr. Hastings' Coinbase account to external locations.

287. Mr. Hastings never authorized the complete depletion of his Coinbase account, which held cryptocurrency worth approximately \$18,600 when Coinbase negligently allowed the account to be emptied.

288. Coinbase now claims Mr. Hastings' Coinbase account has a negative balance.

289. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Hastings has been damaged by the loss of cryptocurrency entrusted with Coinbase.

#### **Mr. Haston's Coinbase Account**

290. Mr. Haston has a Coinbase account.

291. On or about June 21, 2022, Coinbase sent Mr. Haston an email that said "\$2,575.94 will arrive in your bank account by June 24, 2022."

292. That same day, Mr. Haston called Coinbase Support, and informed Coinbase that he did not authorize a withdrawal from his Coinbase account.

293. On June 26, 2022, Mr. Haston received an automated email from Coinbase stating:

If you still require assistance, please reply to this message. If you no longer need help, we will automatically resolve your case in 48 hours.

Thanks,  
Coinbase Support

294. Mr. Haston promptly responded that he still needed assistance, didn't authorize a withdrawal of his funds, and had lost access to his account.

295. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Haston has been damaged by the loss of funds entrusted with Coinbase.

#### **Mr. Hyatt's Coinbase Account**

296. Mr. Hyatt began purchasing cryptocurrencies on Coinbase in 2021.

297. Mr. Hyatt used his login credentials along with two-factor authentication to access his Coinbase account.

298. In March 2022, Mr. Hyatt's Coinbase account held several cryptocurrencies with a total worth of approximately \$53,835.

299. When Mr. Hyatt checked his Coinbase account in September 2022, he discovered all of the cryptocurrencies held in the account had disappeared.

300. Mr. Hyatt then contacted Coinbase Support to find out what happened to his cryptocurrencies.

301. Mr. Hyatt filed a formal complaint with Coinbase.

302. After repeatedly following-up with Coinbase for information, Coinbase informed Mr. Hyatt that Coinbase allowed his account to be accessed on June 27, 2022, from a new device with an entirely different IP location. According to Coinbase, on June 27, 2022, at 1:00 a.m. local time for Mr. Hyatt, Coinbase approved the transfer of approximately \$20,987.87 worth of cryptocurrency from Mr. Hyatt's account to an external location where Mr. Hyatt had never before sent funds.

303. Mr. Hyatt never received a request to approve, never received notice of, and never authorized the above withdrawal or any other undisclosed withdrawals draining his Coinbase account at some point between March and September 2022.

304. Coinbase refuses to tell Mr. Hyatt what happened to his cryptocurrencies. The one unauthorized transaction Coinbase disclosed to Mr. Hyatt, after he contacted Coinbase, does not account for the rest of the value of Mr. Hyatt's Coinbase account, what happened to the rest of Mr. Hyatt's cryptocurrencies, or fees earned by Coinbase from unauthorized transactions in Mr. Hyatt's account.

305. After receiving Mr. Hyatt's formal complaint, Coinbase still refuses to reverse or credit Mr. Hyatt's account for his losses.

306. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Hyatt has been

damaged by the loss of access to his account and the loss of his cryptocurrency holdings entrusted with Coinbase.

### **Mr. Kattula's Coinbase Account**

307. In January 2022, Mr. Kattula opened a Coinbase account and transferred money from his bank account to purchase approximately \$6,000 of cryptocurrency.

308. Mr. Kattula held the cryptocurrency in his Coinbase account.

309. Around April 2022, Mr. Kattula received an email purporting to be from Coinbase requesting that he change his password for security purposes. Mr. Kattula attempted to change his password according to the provided instructions.

310. After his attempt to change his Coinbase password, on or around April 28, 2022, nearly \$6,000 worth of cryptocurrency was drained from Mr. Kattula's Coinbase account and transferred to destinations Mr. Kattula had never sent or received money from. Coinbase authorized the complete depletion of Mr. Kattula's Coinbase account.

311. Coinbase-authorized unknown parties also attempted to purchase additional cryptocurrency "on margin," that is with money borrowed from Coinbase. On April 28, 2022, Coinbase allowed the unauthorized withdrawal of \$1,000 from Mr. Kattula's bank account. Coinbase made that \$1,000 immediately available to

unknown person(s) who promptly purchased \$1,000 in cryptocurrency using Mr. Kattula's account. Mr. Kattula did not authorize the complete depletion of his account nor the \$1,000 withdrawal from his bank account.

312. Upon Mr. Kattula's request, his bank reversed the unauthorized transfer of \$1,000 to Coinbase.

313. In response, Coinbase froze Mr. Kattula's account and treated it as having a negative balance.

314. Coinbase later recovered nearly all of the \$1,000 used to make the unauthorized purchase of cryptocurrency. However, Coinbase refused to compensate Mr. Kattula for all the cryptocurrency stolen from his account.

315. On May 3, 2022, Mr. Kattula filed a formal complaint with Coinbase regarding unauthorized access to Mr. Kattula's account.

316. On or about May 21, 2022, Mr. Kattula received an automated email response from Defendants stating:

"Hello,

Thanks for filing a Formal Complaint with Coinbase.

The Disputes Team is currently looking into your Complaint and we require some additional time to fully investigate and respond to you. Please allow up to 20 business days to fully investigate your complaint and provide you with a Resolution Notice.

Thanks for your patience, we will provide you with a response as soon as possible.

Thank you,  
Coinbase Support.

317. On June 24, 2022, 52 days after he submitted his Formal Complaint, Coinbase sent Mr. Kattula another form email rejecting his “Formal Complaint” and refusing to reimburse him for the unauthorized transactions.

318. In rejecting his complaint, Coinbase admitted the unauthorized transfers from Mr. Kattula’s account on April 28, 2022, were from an IP address that has never been associated with Mr. Kattula and was located far away from the physical location and IP address from which he always accessed his account.

319. Coinbase could have easily identified and prevented losses from the unauthorized activity on Mr. Kattula’s account.

320. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Mr. Kattula has been damaged by the loss of cryptocurrency he entrusted with Coinbase.

### **Ms. Krieser’s Coinbase Account**

321. Ms. Krieser had a Coinbase account in which she held various cryptocurrencies.

322. As Ms. Krieser later discovered, on or about September 6, 2022, Coinbase allowed an unknown person to convert all of the cryptocurrency in Ms. Krieser's Coinbase account into cash. The fees and/or spread for those transactions totaled over \$450.

323. Coinbase then allowed the entire cash balance of Ms. Krieser's Coinbase account - \$32,062.43 – to be emptied to a bank account never before associated with Ms. Krieser's Coinbase account.

324. On or about September 9, 2022, Ms. Krieser alerted Coinbase to the unauthorized transactions in her Coinbase account.

325. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Krieser has been damaged by the loss of her holdings, both cryptocurrency and cash, entrusted with Coinbase.

### **Mr. Larson's Coinbase Account**

326. Mr. Larson had a Coinbase account in which he held cryptocurrency.

327. On or about March 15, 2022, Coinbase allowed a (new) computer operating from an IP address associated with a location in Iowa to access Mr. Larson's Coinbase account. Coinbase then allowed an unknown person to transfer Mr. Larson's cryptocurrency to a Coinbase Pro Account, even though



Mr. Larson had never before subscribed to Coinbase Pro. Next, Coinbase allowed Mr. Larson's approximately \$17,5000 in cryptocurrency to be withdrawn from the Coinbase Pro account to an external location.

328. Mr. Larson did not authorize any of the above transfers or withdrawals.

329. Around that same time, Mr. Larson attempted to lock his Coinbase account. Mr. Larson was unable to immediately lock his Coinbase account, so he promptly contacted Coinbase Support by phone to secure his account and report the unauthorized transactions. Coinbase claimed to have locked Mr. Larson's account on March 15, 2022.

330. Later that day and on March 16, 2022, Coinbase Support sent Mr. Larson multiple emails addressed to someone else. The emails began with: "Hi Linda," and provided automated instructions for accessing a Coinbase account without SMS and addressed eligibility to purchase additional cryptocurrency.

331. Mr. Larson responded, "Hello, I don't know who Linda is, I am not Linda I'm Eric . . ."

332. Mr. Larson then received another incongruous email from Coinbase. This time the email began "Hi there," and began "To complete our security review we need to verify your identity." This email was sent to both Mr. Larson's email address and another email address that began with "linda..." Mr. Larson has no

association with the gmail address copied on messages from Coinbase Support discussing the compromise of his Coinbase Account.

333. Even after Mr. Larson pointed out the error, Coinbase persisted and sent another automated email with a gmail address for a “Linda.”

334. Finally, Coinbase stopped emailing the gmail address for “Linda,” but never explained the added addressee on the emails or the connection of “Linda” to Mr. Larson’s Coinbase Account.

335. On or about March 15, 2022, Coinbase also allowed an unknown person to request \$1,000 from Mr. Larson’s linked bank account. Mr. Larson’s bank reversed that transaction after Mr. Larson reported it was not authorized by him.

336. Coinbase refused to refund or credit Mr. Larson for the cryptocurrency Coinbase allowed to be taken from his account.

337. Rather, Coinbase claimed Mr. Larson owed Coinbase for the chargeback caused by his bank reversing the unauthorized withdrawal from Mr. Larson’s bank. To recoup that amount, Coinbase seized a portion of Mr. Larson’s cryptocurrency.

338. Mr. Larson has called Coinbase numerous times regarding the unauthorized transactions, but each time Coinbase failed to resolve anything.

339. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Larson lost approximately \$17,500 worth of cryptocurrencies wrongfully seized by Coinbase.

### **Mr. Longstreth's Coinbase Account**

340. Mr. Longstreth had a Coinbase Account.

341. On or around September 12, 2022, Mr. Longstreth noticed over \$8,000 of funds missing from his Coinbase account.

342. Mr. Longstreth immediately contacted his banks to freeze any transactions.

343. One of Mr. Longstreth's banks was able to freeze an unauthorized transaction for \$7,500.

344. Coinbase then restricted Mr. Longstreth's account. According to Coinbase, Mr. Longstreth's account was restricted because of an outstanding balance resulting from the bank's reversal of the aforementioned transaction.

345. Mr. Longstreth notified Coinbase about the unauthorized transactions in his Coinbase account.

346. Apparently, despite his loss of thousands of dollars, Mr. Longstreth now "owes" Coinbase for an unauthorized transaction that would have never

occurred but for Coinbase's lax security measures and nonsensical banking procedures.

347. Coinbase has refused to reverse or credit Mr. Longstreth for the cryptocurrency lost from his Coinbase account.

348. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Longstreth lost thousands of dollars' worth of cryptocurrency entrusted with Coinbase. Additionally, Coinbase demands that Mr. Longstreth pay it the outstanding balance on his account.

### **Mr. Mang's Coinbase Account**

349. Mr. Mang held cryptocurrency in his Coinbase account.

350. On August 5, 2022, Mr. Mang received an email purportedly from Coinbase requesting that he verify his identity and he attempted to do so.

351. That same day, Mr. Mang also promptly called Coinbase Support to secure his account. Coinbase assured Mr. Mang his account was secure.

352. Later, Mr. Mang learned from Coinbase that Coinbase had authorized the complete depletion of his account on August 5, 2022, through a series of about 18 transactions. These transactions included the conversion of cryptocurrencies in Mr. Mang's account.

353. Approximately \$51,674 in cash (U.S.D.) was withdrawn from Mr. Mang's Coinbase account to bank accounts without his authorization.

354. Approximately \$151.59 worth of cryptocurrency was withdrawn from Mr. Mang's Coinbase account and sent to an external location.

355. Mr. Mang did not authorize the transactions on August 5, 2022, or the draining of his account.

356. Coinbase failed to delay or stop the processing and execution of the above suspicious activity on Mr. Mang's account.

357. Coinbase refused to reverse or credit the unauthorized transfers of cash from Mr. Mang's account.

358. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result, Mr. Mang has been damaged by the loss of funds and cryptocurrency from his Coinbase account.

#### **Ms. Marcial's Coinbase Account**

359. Ms. Marcial held cryptocurrency in her Coinbase account.

360. On July 3, 2022, Coinbase permitted the addition of a new (unauthorized) device to Ms. Marcial's Coinbase account.

361. On July 4, 2022, several unauthorized transactions were made in Ms. Marcial's account.

362. And Ms. Marcial's debit card was used to make four unauthorized purchases of USDC. When these charges were reversed by Ms. Marcial's bank, Coinbase placed a hold on her Coinbase account and demanded she pay Coinbase \$195.78.

363. That same day, Coinbase allowed Ms. Marcial's account to be drained in three unauthorized transactions totaling \$6,260.26. Coinbase authorized the transfers to a MetaBank debit card issued in someone else's name, not the account holder's name.

364. On July 4, 2022, Ms. Marcial immediately contacted Coinbase Customer Service and notified them of the unauthorized transactions. Coinbase informed her that there was nothing that could be done since the withdrawals were, according to Coinbase, already completed. However, the withdrawal notice from Coinbase stated the funds would arrive in the destination bank account by July 8, 2022.

365. Ms. Marcial called Coinbase on July 6, 2022, to request the complete name and debit card number for the MetaBank Card used to withdraw funds. Coinbase could not release more than the last four digits of the debit card number and could not release the complete name associated with the debit card. Coinbase instructed Ms. Marcial to call MetaBank for that information.

366. On July 21, 2022, Ms. Marcial submitted a customer service complaint to Coinbase asking Coinbase (again) to reverse the unauthorized transactions in her account. Ms. Marcial followed-up with Coinbase on July 22, 2022, and was informed that her dispute was escalated to another level. A month passed, yet Coinbase still did not respond to Ms. Marcial.

367. Ms. Marcial contacted Coinbase again on or about August 24, 2022. She submitted a “Formal Complaint” by certified mail to the UPS Store in New York where Coinbase receives direct complaints. Ms. Marcial has never received a response from Coinbase to her Formal Complaint.

368. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Ms. Marcial has lost cryptocurrency and funds entrusted with Coinbase.

### **Ms. McWilliams’ Coinbase Account**

369. Ms. McWilliams held cryptocurrency in a Coinbase Pro account.

370. On or about August 24, 2022, Ms. McWilliams’ cryptocurrency was converted into cash. Ms. McWilliams did not authorize those transactions.

371. That same day, Coinbase sent Ms. McWilliams an email informing her that “A withdrawal of \$12,253.98 has been started” and that “\$12,253.98 will arrive

in your bank account by August 29, 2022.” Ms. McWilliams did not authorize the withdrawal of all the cash from her Coinbase account to an external account.

372. Ms. McWilliams notified Coinbase that the above transactions were not authorized by her.

373. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Ms. McWilliams has been damaged by the loss of her cryptocurrency entrusted with Coinbase.

#### **Mr. Mechanic’s Coinbase Account**

374. Mr. Mechanic had a Coinbase and Coinbase Pro account containing various cryptocurrencies.

375. On February 11, 2022, Coinbase approved a withdrawal of \$6,596.27 from Mr. Mechanic’s account.

376. Mr. Mechanic informed Coinbase he did not authorize that transaction. Coinbase failed to provide a substantive response to Mr. Mechanic.

377. The “Account History” of Mr. Mechanic’s Coinbase account no longer shows the unauthorized transaction depleting his account. Coinbase has failed to display, or has even deleted, the records of fraudulent transactions from his account history.



378. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Mechanic lost thousands of dollars of funds entrusted with Coinbase.

### **Mr. Mihalitsas's Coinbase Account**

379. In April 2022, Mr. Mihalitsas's bank reversed an unauthorized transfer of \$500.00 to his Coinbase exchange account after his debit card number had been compromised.

380. In response, Coinbase froze his Coinbase account until he reimbursed Coinbase for that \$500.00. Coinbase threatened to seize Mr. Mihalitsas's cryptocurrency if he did not pay that amount to Coinbase.

381. Mr. Mihalitsas paid the \$500.00 Coinbase demanded, even though the chargeback was the result of an unauthorized transaction. Coinbase acknowledged receipt of that payment in an email.

382. However, when Mr. Mihalitsas contacted Coinbase to regain access to his account, he was told to allow 30 days for his account to be restored – i.e., to wait until early May 2022.

383. Mr. Mihalitsas's account has not been restored since then. He has been locked out of his Coinbase account for several months – despite repeatedly

contacting Coinbase Support and attempting to complete Coinbase's ID verification process.

384. When Mr. Mihalitsas asks Coinbase why they won't open his account, Coinbase simply responds that they cannot tell him why. In one message, Coinbase stated: "There are a number of factors that affect purchase and eligibility to add cash, and we're not able to provide specific details regarding our security processes or account reviews."

385. Mr. Mihalitsas has filed a Formal Complaint with Coinbase but remains unable to access his account, despite complying with Coinbase's various requests.

386. As a result of Coinbase's conduct, Mr. Mihalitsas is unable to buy or sell on Coinbase's exchange, which is one of the few licensed money transmitters handling virtual currency in New York.

### **Mr. Nessler's Coinbase Account**

387. Mr. Nessler held cryptocurrency in his Coinbase Account.

388. He has been locked-out of his Coinbase account since January 4, 2022.

389. On or about January 4, 2022, Mr. Nessler's Coinbase account of cryptocurrency worth approximately \$65,000 at the time, was completely drained by an unauthorized third-party.

390. Coinbase also allowed an unauthorized third-party to purchase Bitcoin by withdrawing money from Mr. Nessler's bank account.

391. On top of losing his cryptocurrency and losing access to his account, Coinbase claims Mr. Nessler owes it around \$800 because Mr. Nessler's bank reversed the unauthorized withdrawals from Mr. Nessler's bank account.

392. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Nessler has lost access to his Coinbase account and has lost cryptocurrency entrusted with Coinbase.

#### **Mr. Onimus's Coinbase Account**

393. Mr. Onimus opened a Coinbase Pro account around February 2021.

394. Mr. Onimus made a number of deposits into the account thereafter, which he used to purchase cryptocurrencies.

395. During the summer of 2021, Mr. Onimus attempted to make additional deposits into his Coinbase Pro account but was unable to and shortly after received messages from Coinbase stating "Deposits Disabled."

396. Mr. Onimus attempted to rectify this problem numerous times by contacting Coinbase and complying with their requests, including uploading his photo ID.

397. At that time, Mr. Onimus was unable to get in touch with “live” person at Coinbase. Coinbase only provided automated responses to his requests for help.

398. On or about January 4, 2022, Mr. Onimus tried again to deposit additional funds into his Coinbase Pro account, but he again received the same error message from Coinbase: “Deposits Disabled.”

399. On or about January 4, 2022, Mr. Onimus received an email from Coinbase advising him of a withdrawal from his account. Mr. Onimus immediately notified Coinbase of the unauthorized transaction and requested to secure his account.

400. Mr. Onimus learned that Coinbase had authorized the transfer of approximately \$13,000 in cryptocurrency, to an external location. Mr. Onimus did not initiate that transfer, which drained his entire Coinbase Pro Account.

401. Coinbase refused to reverse or credit Mr. Onimus’ account for his loss.

402. Mr. Onimus filed a “Formal Complaint” using Coinbase’s online form on January 21, 2022, and emailed Coinbase Support that same day informing them he had submitted a “Formal Complaint” online.

403. After submitting his “Formal Complaint” with Coinbase online, Coinbase displayed the following screen, indicating a “high number of requests” were overwhelming Coinbase and discouraging Mr. Onimus from contacting banks:

## Success

Thanks for taking the time to contact us. We're currently receiving a high number of requests so we may take longer to respond, but our team is working hard to get to every inquiry quickly.

We'll get in touch with you as soon as we can. In the meantime, please do not submit another inquiry for the same request as this causes further delays. Please also **do not contact our partner banks**, as they will be unable to assist you since your account is managed by Coinbase.

We appreciate your patience and look forward to helping you!

404. On February 7, 2022, Mr. Onimus received an email from Coinbase Support stating:

Hi,

Thanks for working with Coinbase Support.

We hope you were able to get the help you needed. We're closing this case; if you need additional support, please visit the Coinbase Help Center for quick answers to many questions.

Regards,  
Coinbase Support

405. On February 8, 2022, Coinbase sent Mr. Onimus another email, with a new "Case#" in the email subject, refusing to compensate him for the unauthorized transaction in his account.

406. Mr. Onimus never received an email or other written communication directly from Coinbase that was described as a response to his “Formal Complaint.”

407. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase’s conduct, Mr. Onimus has been damaged by the loss of his cryptocurrency entrusted with Coinbase.

### **Ms. Pillai’s Coinbase Account**

408. Ms. Pillai held cryptocurrency in her Coinbase account.

409. On August 29, 2022, Coinbase sent Ms. Pillai an email stating that Coinbase had authorized the transfer of cryptocurrency worth approximately \$5,200 from Ms. Pillai’s Coinbase Account to a destination where Ms. Pillai had never before sent funds or cryptocurrency.

410. Coinbase’s email alerting Ms. Pillai of the transfer added, “If this wasn’t you, lock your account immediately. Not you? [Lock your account.](#)”

411. Ms. Pillai promptly notified Coinbase that she did not authorize the above-referenced transaction draining her account.

412. Coinbase has refused to reverse or credit Ms. Pillai for the cryptocurrency taken from her account.

413. Despite attempting multiple times to comply with Coinbase's requirements, Ms. Pillai has been unable to regain access to her Coinbase account or the cryptocurrencies that may remain.

414. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Pillai has been damaged by the loss of access to her account and the loss of her cryptocurrency holdings entrusted with Coinbase.

#### **Mr. Plyler's Coinbase Account**

415. In December 2017, Mr. Plyler purchased and held cryptocurrencies in his Coinbase Account.

416. On January 16, 2018, Mr. Plyler purchased and held additional cryptocurrency in his Coinbase Account. After that, there were no transactions in Mr. Plyler's Coinbase account, until the unauthorized transactions occurring in December 2021.

417. Mr. Plyler never sold, converted, or transferred anything held in his Coinbase Account.

418. On or about December 12, 2021, Mr. Plyler became aware of unauthorized attempts to access his Coinbase account. Mr. Plyler immediately notified Coinbase of the issue and requested Coinbase secure and lock his account.

419. Coinbase did not follow Mr. Plyler's instructions. Coinbase permitted a third-party to access Mr. Plyler's Coinbase account from a new device, at a new IP address, and from a new location.

420. Later, Coinbase approved requests to convert Mr. Plyler's cryptocurrencies. Mr. Plyler did not authorize these transactions either.

421. Coinbase collected fees for the above unauthorized conversions.

422. After Mr. Plyler instructed Coinbase to lock and secure his account, Coinbase approved a transfer of the full balance of cryptocurrency from his Coinbase account. Again, Mr. Plyler did not authorize this transaction.

423. Mr. Plyler continued to communicate with Coinbase support. He informed Coinbase he had not approved the draining of his account, which he explained occurred after he instructed Coinbase to lock his account. Coinbase Support replied with automated messages, containing contradictory information about what happened in Mr. Plyler's Coinbase account.

424. The emails from Coinbase provided a link to submit an additional support request to Coinbase (not a direct link to the Formal Complaint form on Coinbase's website) and directed "less formal legal documents" to a Coinbase Legal, PO Box in San Francisco, California.



425. Mr. Plyler's Coinbase account transaction history shows the unauthorized conversions of several cryptocurrencies. Further, despite the fact that Mr. Plyler's Coinbase account had been completely drained, his account's transaction history does not show the unauthorized transaction.

426. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Plyler lost the entire balance of his Coinbase Account, which was then worth approximately over \$2,000.

#### **Mr. Polhill's Coinbase Account**

427. Mr. Polhill relied upon Coinbase's representations that its platform was secure when deciding to use it to purchase and store cryptocurrencies.

428. On or about December 1, 2021, and late at night, Coinbase sent Mr. Polhill an email stating that his password had been reset. The next morning, when Mr. Polhill read the email hours later, he immediately took steps to secure his Coinbase account.

429. Mr. Polhill learned from his cell phone provider that his cell phone's SIM card had been "swapped" at a store in California, allowing an unknown thief to receive calls and text messages to Mr. Polhill's cell phone number.

430. Mr. Polhill had never accessed his Coinbase account from California.

431. Nonetheless, Coinbase allowed an unknown person using a device with an IP address indicating its location was in California to completely deplete Mr. Polhill's Coinbase account of over \$5,000 worth of cryptocurrency.

432. On December 1, 2021, Mr. Polhill notified Coinbase that the transfers draining his account of cryptocurrency were completely unauthorized.

433. Mr. Polhill has complied with Coinbase's instructions for regaining access to his account but has been unable to regain access to his Coinbase account.

434. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Polhill has been damaged by the loss of access to his account and the loss of his cryptocurrency holdings entrusted with Coinbase.

#### **Mr. Paperno's Coinbase Account**

435. Mr. Paperno held cryptocurrency in a Coinbase account.

436. On or about September 2, 2021, Coinbase allowed a withdrawal of approximately over \$28,000 worth of cryptocurrency from Mr. Paperno's Coinbase account.

437. Mr. Paperno never authorized the above withdrawals from his Coinbase account.

438. Mr. Paperno spent weeks calling Coinbase numerous times but has not received a satisfactory response from Coinbase.

439. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Paperno has been damaged by the loss of cryptocurrency entrusted with Coinbase.

### **Mr. Rodriguez's Coinbase Account**

440. Mr. Rodriguez had a Coinbase account in which he held cryptocurrency.

441. On or about May 14, 2021, Coinbase allowed an unknown third-party to change the email address on Mr. Rodriguez's account.

442. Coinbase also allowed the unknown third-party to empty Mr. Rodriguez's account and to attempt a \$10,000 transfer from Mr. Rodriguez's bank account to his Coinbase account, which was rejected by Mr. Rodriguez's bank.

443. Due to the unauthorized attempt to transfer money from Mr. Rodriguez's bank account, Coinbase threatened to sell any remaining holdings in Mr. Rodriguez's Coinbase account and restricted Mr. Rodriguez's Coinbase account.

444. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Rodriguez has

been damaged by the loss of approximately \$10,000 in cryptocurrency entrusted with Coinbase.

### **Mr. Samuel's Coinbase Account**

445. On or about September 14, 2022, at 2:58 p.m., Coinbase emailed Mr. Samuel that a purchase of cryptocurrency worth approximately \$1,000 was “declined” “[d]ue to a suspicious activity warning.”

446. Mr. Samuel did not authorize that attempted purchase.

447. However, two minutes later, Coinbase allowed the purchase of \$499.00 worth of cryptocurrency using payment from the same linked financial account. Coinbase's fee or “spread” for this purchase was approximately \$19.15.

448. Mr. Samuel did not authorize that purchase either.

449. He promptly notified Coinbase of the unauthorized activity and requested Coinbase secure his account. When attempting to contact Coinbase, Mr. Samuel was unable to reach a ‘live’ support person.

450. Coinbase allowed at least two withdrawals of cryptocurrency worth over \$500 from Mr. Samuel's account to an external location.

451. Coinbase emailed Mr. Samuel that additional attempts to purchase cryptocurrency from his account were cancelled. Mr. Samuel had not authorized those attempted purchases either.

452. In response to Mr. Samuel's support request, Coinbase later emailed him:

Hi,

Thanks for working with Coinbase Support.

We hope you were able to get the help you needed. We're closing this case; if you need additional support, please visit the Coinbase Help Center for quick answers to many questions.

Regards,  
Coinbase Support

453. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Samuel has been damaged by the loss of funds and cryptocurrency entrusted with Coinbase.

**Mr. Sims' Coinbase Account and Coinbase Wallet Account**

454. Mr. Sims had a Coinbase account and a Coinbase Wallet Account holding various cryptocurrencies and NFT's, or non-fungible tokens.

455. Mr. Sims never shared any login credentials associated with his Coinbase account and had two-factor authentication in place to further safeguard his assets.

456. According to Coinbase's records, on or about July 8, 2022, at around 1:44 am California time, Coinbase allowed the cryptocurrency in Mr. Sims's Coinbase account to be withdrawn and sent to external locations.

457. From May 2022 to June 2022, Mr. Sim's Coinbase Wallet was breached multiple times, resulting in a further loss of his cryptocurrency.

458. On or around August 5, 2022, Mr. Sims contacted Coinbase directly to report the unauthorized transactions.

459. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Sims has been damaged by the loss of his cryptocurrency entrusted with Coinbase.

#### **Mr. Sowell's Coinbase Account**

460. Mr. Sowell had a Coinbase Account in which he stored various cryptocurrencies.

461. On or about June 27, 2022, Coinbase allowed the access of Mr. Sowell's Coinbase account, the conversion of his cryptocurrency to cash, and the complete depletion of funds in his account. Approximately \$1,814.78 (U.S.D.) of funds were withdrawn from Mr. Sowell's Coinbase account to a newly added external account.

462. Mr. Sowell informed Coinbase that these withdrawals from his Coinbase account were unauthorized.

463. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Sowell has been

damaged by the loss of his cryptocurrency and funds entrusted with Coinbase in his account.

### **Ms. Spassova's Coinbase Account**

464. Ms. Spassova had a Coinbase account holding cryptocurrency.

465. On or about August 17, 2022, Ms. Spassova instructed Coinbase to lock and secure her Coinbase account to prevent any unauthorized transactions.

466. Coinbase failed to lock and secure Ms. Spassova's account as she expressly instructed.

467. According to an email from Coinbase, on or about August 18 through August 19, Coinbase authorized other person(s) – operating from three different IP addresses associated with locations far from where Ms. Spassova lives and uses Coinbase – to access and drain Ms. Spassova's Coinbase account.

468. Coinbase approved the transfer of over \$18,000 (U.S.D.) cash from Ms. Spassova's account to three different (newly added) accounts at banks in the United States. Ms. Spassova does not have an account in her name at any of the banks where the funds were sent without her authorization. The accounts and banks where Coinbase authorized the funds to be sent were never previously associated or connected with Ms. Spassova's Coinbase account.

469. Ms. Spassova promptly notified Coinbase that she did not authorize the above-referenced unauthorized transactions in her account or the depletion of cash from her account.

470. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Spassova has been damaged by the loss of funds entrusted with Coinbase.

#### **Mr. Stefani's Coinbase Wallet Account**

471. Mr. Stefani had a Coinbase Wallet account in which he held cryptocurrency.

472. On or about August 15, 2022, over approximately \$235,000 worth of cryptocurrency was transferred from Mr. Stefani's Coinbase Wallet.

473. Mr. Stefani did not authorize those transactions.

474. Mr. Stefani promptly informed Coinbase that he did not authorize the withdrawals from his Coinbase Wallet Account.

475. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Stefani has been damaged by the loss of cryptocurrency entrusted with Coinbase.



### **Mr. Suero's Coinbase Account and Coinbase Wallet Account**

476. Mr. Suero had a Coinbase account and a Coinbase Wallet Account holding several different cryptocurrencies.

477. On or about October 13, 2019, Mr. Suero's Coinbase Wallet Account was liquidated when his cryptocurrency was converted and then withdrawn from his Coinbase Wallet Account. Mr. Suero did not authorize these transactions.

478. Mr. Suero notified Coinbase of the unauthorized transactions in his Coinbase Wallet account.

479. One of the unauthorized transactions no longer appears in Mr. Suero's account transaction history.

480. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result Coinbase's conduct, Mr. Suero has been damaged by losing cryptocurrency then worth approximately \$454.44.

### **Mr. Tucker's Coinbase Account**

481. Mr. Tucker had a Coinbase account in which he was holding cash on July 13, 2022.

482. On July 13, 2022, Mr. Tucker received an email purporting to be from Coinbase and threatening to restrict his account (as Coinbase is infamous for doing)

if he did not verify his information. Mr. Tucker attempted to comply with the request.

483. Within hours of doing so, Mr. Tucker separately contacted Coinbase Support to make sure his account was secure.

484. Coinbase Support informed him that a third-party had gained unauthorized access to his Coinbase account. The unauthorized third-party accessed Mr. Tucker's Coinbase account from an IP address identified as being located in Batam, Indonesia. Coinbase permitted this unauthorized third-party to add a new payment method to Mr. Tucker's account. When it was around 3:00 a.m. on July 13 in Batam, Indonesia, Coinbase allowed the unauthorized third-party to withdraw the entire cash balance of \$4,495.95 (U.S.D.) in Mr. Tucker's account to the newly added account.

485. Mr. Tucker always accessed his Coinbase account from his own device or devices, and from the United States.

486. Mr. Tucker always used the same payment method to transfer funds to his Coinbase account.

487. Cryptocurrencies cannot legally be used for payments in Indonesia.

488. After Mr. Tucker notified Coinbase the transactions in his account were not authorized by him, Coinbase provided Mr. Tucker with one of its automated responses:

Unfortunately, as you may already be aware, all cryptocurrency transactions are irreversible once they've been confirmed on their respective blockchain and the funds are not able to be recovered by Coinbase.

489. Coinbase's response to Mr. Tucker that the unauthorized transaction was an irreversible "cryptocurrency transaction" was false based on the information Mr. Tucker was given by Coinbase itself.

490. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase conduct, Mr. Tucker has been damaged by the loss of funds entrusted with Coinbase.

#### **Ms. Waheed's Coinbase Account**

491. Ms. Waheed had a Coinbase and Coinbase Pro account.

492. On or about June 2022, Ms. Waheed discovered all of her cryptocurrency had been sold and withdrawn from her Coinbase account. Ms. Waheed learned that, from May 1, 2022, to May 6, 2022, the cryptocurrency in her Coinbase Pro account had been transferred to her Coinbase account, and then ultimately withdrawn.

493. Coinbase allowed \$113,863.84 (U.S.D.) in cash to be withdrawn from Ms. Waheed's Coinbase account to an account based in Utah that had never before been associated with Ms. Waheed's account.

494. Ms. Waheed did not authorize the withdrawal and notified Coinbase of this unauthorized transaction.

495. To make matters worse, Coinbase has consistently interrupted Ms. Waheed's account access by locking and then unlocking her ability to access her account.

496. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Waheed has been damaged by the loss of access to her account and the loss of her account holdings entrusted with Coinbase.

#### **Mr. White's Coinbase Account**

497. Mr. White had a Coinbase account and Coinbase Pro account.

498. Mr. White traveled around the country, including in New York, as a front-line worker during the peak of the Covid-19 pandemic in early 2020. He deposited his savings from this hard work into his Coinbase accounts.

499. Coinbase provided Mr. White with a Coinbase Card. The Visa Debit Card was issued by MetaBank and “powered by Marqeta” but Coinbase purportedly provides the customer service for the card.

500. Mr. White treated his Coinbase accounts as his checking and savings accounts.

501. On December 1, 2021, after a long assignment, Mr. White received an email indicating his Coinbase account had been compromised. He did not click on the alert, and everything seemed to be normal when he checked his account in the Coinbase App.

502. Then, Mr. White received a series of back-to-back calls purportedly from Coinbase, indicating that his account needed to be secured by entering in a series of numbers. Mr. White eventually answered and obliged with the requests of the caller.

503. Mr. White never disclosed his password.

504. Less than an hour later, Mr. White discovered he was unable to login to his Coinbase accounts.

505. Mr. White immediately attempted to call Coinbase. After great effort, Mr. White found a telephone number for Coinbase and called them about problems with his account. Coinbase advised Mr. White that it would refund any money he

had lost and advised him to change the password for his email account, which he did.

506. The next day, on December 2, 2021, Coinbase locked Mr. White's account. On December 22, 2021, Coinbase stated that he had a negative account balance, and his account access could not be restored until he paid approximately \$2,071.58 from a bank account linked to Coinbase via Plaid.

507. Mr. White informed Coinbase that withdrawals draining his Coinbase account and Coinbase Pro account were unauthorized transactions.

508. Mr. White has not been able to regain access to his Coinbase accounts since.

509. Coinbase refuses to even provide Mr. White with a record of his account transactions.

510. On January 23, 2022, Mr. White submitted a "Formal Complaint" to Coinbase.

511. On February 4, 2022, Coinbase sent an email at 2:33 a.m. in response to Mr. White's "complaint." Coinbase stated in an automated or template email that it determined Mr. White was not eligible to be reimbursed for a transfer of "funds" from his account "on 1 December 2021."

512. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. White has been damaged by the loss of access to his account and the loss of funds entrusted with Coinbase.

### **Mr. Whittington's Coinbase Account**

513. Mr. Whittington had a Coinbase Pro account in which he held cryptocurrency.

514. On or about September 24, 2022, Mr. Whittington's Coinbase Pro account was breached by an unknown person and the cryptocurrency in it transferred from Mr. Whittington's Coinbase Pro account to his Coinbase account.

515. Mr. Whittington communicated with Coinbase Support to secure his account and followed Coinbase's instructions to verify his identity.

516. However, soon thereafter, Coinbase allowed the withdrawal of approximately \$47,000 worth of cryptocurrency from Mr. Whittington's Coinbase account.

517. Mr. Whittington did not authorize those withdrawals from his Coinbase account, which emptied or nearly emptied the account.

518. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Whittington has

been damaged by the loss of his cryptocurrency worth almost \$50,000 (U.S.D.) entrusted with Coinbase.

### **Ms. Wright's Coinbase Account**

519. Ms. Wright had a Coinbase account in which she stored cryptocurrency.

520. On September 1, 2022, Coinbase allowed an unknown person(s) to access Ms. Wright's Coinbase account and setup a new two-factor authentication process.

521. Coinbase alerted Ms. Wright that a new phone number had been added to her account. Ms. Wright was then unable to access her Coinbase account. She promptly contacted Coinbase to address the problem.

522. At the same time, without Ms. Wright's authorization or knowledge, a new debit card was added to Ms. Wright's account. According to a Coinbase Support representative, several transactions withdrawing thousands of dollars from Ms. Wright's account onto the new fraudulent debit card were initiated by an unknown person and approved by Coinbase. Coinbase would not reveal further details about the fraudulent debit card.

523. According to Coinbase, approximately over \$7,000 worth of cryptocurrency and cash were withdrawn from her Coinbase account.



524. Later, Ms. Wright received in the mail, a Coinbase Card from Coinbase without any terms provided alongside it.

525. In an effort to regain access to her Coinbase account, Ms. Wright followed the identity verification instructions provided by Coinbase. However, despite doing so, she has not been able to regain access to her Coinbase account. Coinbase has also refused to reverse or credit Ms. Wright for the funds she lost from her account.

526. Ms. Wright submitted a formal complaint to Coinbase.

527. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Wright has been damaged by the loss of access to her account and the loss of her account holdings, both cryptocurrency and funds, entrusted with Coinbase.

### **B. Coinbase's Flawed User Interface Allows Thefts from Coinbase Wallet Accounts**

528. The Coinbase Wallet Twitter account boldly describes the Coinbase Wallet as "The easiest and most secure crypto wallet and dapp browser." *See* <https://twitter.com/CoinbaseWallet>. The Coinbase website promotes the Wallet as a way to "safely store your crypto," "[U]se DeFi liquidity pools to supply or borrow crypto," "[S]wap assets on decentralized exchanges," and as supporting "a whole world of decentralized apps." *See* <https://www.coinbase.com/wallet>.

529. Unlike centralized exchanges (which use a market-maker system similar to how stocks are traded), decentralized finance (“DeFi”) exchanges operate without a third-party in the middle. So-called “smart contracts” (a computer program that automatically executes) built into the DeFi exchanges determine the price of cryptocurrencies being exchanged and execute trades for the two counterparties.

530. Because DeFi exchanges operate without a third-party in the middle, they rely on crowd-sourced liquidity pools to supply capital for trades of cryptocurrencies handled by the DeFi exchange. Owners of cryptocurrency lend their cryptocurrency to the liquidity pool under the terms of a smart contract, and in return, the DeFi exchange rewards them with a percentage of the trading fees from the pool, which percentage can be based on the cryptocurrency owner’s share of that liquidity pool.

531. The only way to interact with DeFi exchanges and to participate in a liquidity pool (whether as an investor or someone seeking to exchange cryptocurrencies) is through a non-custodial wallet, such as the Coinbase Wallet. Within the Coinbase Wallet, users can access liquidity mining pools through what is called a decentralized application (or a “dapp”).

532. There are legitimate liquidity mining pools, but scammers have also created fake crypto liquidity mining pools. These scammers direct individuals specifically to the Coinbase Wallet because scammers know that they can more easily exploit Coinbase's lax security and defective design. Then, in the Coinbase Wallet, the user is told to purchase a "voucher" or "mining certificate" for a relatively low price.

533. In these scams, the vouchers are in fact a malicious smart contract that gives the scammers indefinite and unlimited access to all the funds in the user's Coinbase Wallet Account. The "smart contract" lurks in the user's Coinbase Wallet Account while the user is induced to amass a large amount of cryptocurrency in his or her Coinbase Wallet Account. Instead of warning users that the Coinbase Wallet's code is granting the unlimited spend access under the smart contract, the Coinbase Wallet provides no notification of this hidden authority. Rather, the Coinbase Wallet presents the payment for the voucher as a one-time transaction, asking the user to "confirm payment" and approve "an action."

534. Unlike the Coinbase Wallet, the MetaMask Wallet, for example, allows users to see and edit the "spend limit permission" of a given smart contract.

535. Coinbase has been aware of flaws of the Coinbase Wallet for at least many months but neglects to protect users from them. Coinbase has also been aware

of specific malicious dapps but failed to warn users about them or delayed in warning users.

### **Mr. Houzenga's Coinbase Wallet Account**

536. In connection with his Coinbase Wallet Account, Mr. Houzenga used a software program called Google Authenticator to secure his Coinbase Wallet. Google Authenticator is a two-factor authentication software Coinbase recommends to its users. The software displays a one-time authentication code a user must enter when logging into an associated account, such as a Coinbase Wallet.

537. In addition, Mr. Houzenga's Coinbase Wallet was secured by a recovery phrase. Coinbase explains:

A recovery phrase (sometimes known as a seed phrase) is a series of words generated by your cryptocurrency wallet that gives you access to the crypto associated with that wallet. Think of a wallet as being similar to a password manager for crypto, and the recovery phrase as being like the master password. As long as you have your recovery phrase, you'll have access to all of the crypto associated with the wallet that generated the phrase — even if you delete or lose the wallet.

538. The Coinbase Wallet Terms of Service Agreement states that “Your Recovery Phrase is the only way to access the cryptocurrency associated with your Wallet App Account.”

539. Mr. Houzenga never shared any login credentials associated with his Coinbase account. He kept his recovery phrase in a secure location that only he has

ever accessed. He has only ever entered the two-factor authentication codes displayed on Google Authenticator when logging into his Coinbase Wallet.

540. When deciding to safeguard his assets in a Coinbase Wallet, Mr. Houzenga relied on Coinbase's representations about the security of its Coinbase Wallet.

541. Through a third-party promotion he was introduced to on the Internet, Mr. Houzenga was promised interest on balances stored in his Coinbase Wallet, if he paid a \$30 initiation fee. Mr. Houzenga paid the fee and indeed received a number of interest payments in his Coinbase Wallet.

542. On July 1, 2022, over \$30,000 worth of Tether (USDT), a cryptocurrency "stablecoin" with a value connected to the U.S. dollar, was transferred out of Mr. Houzenga's Coinbase Wallet. Mr. Houzenga never knowingly authorized or confirmed that transaction from his Coinbase Wallet.

543. Mr. Houzenga reported the unauthorized transaction to Coinbase. On or about July 11, 2022, Coinbase Support refused to refund Mr. Houzenga the amount he lost from his Coinbase Wallet, recommended Mr. Houzenga delete his Coinbase Wallet, and provided him the following generic response:

If you did not confirm any outgoing transactions from your Wallet, we regret to inform you that this means the funds and the seed phrase are now compromised.

We are unable to provide specific details on how your Wallet was compromised. Cryptocurrency transactions are part of an external process, outside of the control of one entity. They cannot be reversed once they are confirmed on the blockchain, therefore Coinbase cannot recover the funds in these instances.

544. As a result of Coinbase's conduct, Mr. Houzenga has been damaged by the loss of funds from his Coinbase Wallet Account.

### **Mr. Gambell's Coinbase Wallet Account**

545. Mr. Gambell held cryptocurrency in his Coinbase Wallet Account, including the stablecoin Tether (USDT), and he also had a Coinbase Account.

546. On or about July 2022, Mr. Gambell interacted with a decentralized application called "datastewards" in the Coinbase Wallet browser.

547. Then, approximately \$140,000 worth of cryptocurrency was drained from Mr. Gambell's Coinbase without him knowingly authorizing withdrawals. Mr. Gambell never received a warning that could happen. Mr. Gambell apparently unknowingly entered into a smart contract with the "datastewards" decentralized application allowing such withdrawals because he never knowingly authorized the emptying of his Coinbase Wallet.

548. Mr. Gambell notified Coinbase of the unauthorized transactions in his Coinbase Wallet Account.

549. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct and defective Coinbase Wallet, Mr. Gambrell lost approximately \$140,000 worth of cryptocurrency.

### **Ms. Dallalnejad's Coinbase Wallet Account**

550. Ms. Dallalnejad held cryptocurrency in her Coinbase Wallet Account, including the stablecoin Tether (USDT).

551. On or about July 2022, while in the Coinbase Wallet application, Ms. Dallalnejad interacted with a decentralized application (dapp) known as ParvestaPD. Ms. Dallalnejad unknowingly entered into a "smart contract" that allowed the dapp to withdraw and irrevocably keep USDT cryptocurrency from Ms. Dallalnejad's Coinbase Wallet Account without her authorization.

552. Ms. Dallalnejad later discovered she had lost full control of her cryptocurrency and could not get it back from the dapp.

553. Ms. Dallalnejad reported to Coinbase the loss and the malicious dapp accessible from the Coinbase Wallet.

554. Even after Ms. Dallalnejad reported the malicious ParvestaPD dapp to Coinbase, the dapp remained accessible (without a warning) in the Coinbase Wallet.

555. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Dallalnejad has

been damaged by losing approximately \$400,000 of cryptocurrency from her Coinbase Wallet Account.

### **Mr. Johnson's Coinbase Wallet Accounts**

556. Mr. Johnson held cryptocurrency in his Coinbase Wallet Accounts.

557. Mr. Johnson used the Coinbase Wallet to interact with decentralized applications (“dapps”), including cbb.vip.

558. Coinbase told Mr. Johnson they would flag cbb.vip as a malicious dapp, but Coinbase did not do so promptly.

559. On or about July 1, 2022, Coinbase allowed approximately \$12,000 worth of USDT cryptocurrency to be withdrawn from Mr. Johnson's Coinbase Wallet Account, without his express permission for an irrevocable withdrawal.

560. Separately this year, Mr. Johnson lost approximately \$100,000 worth of cryptocurrency when Coinbase allowed withdrawals from Mr. Johnsons Coinbase Wallet Account, without his express permission for an irrevocable withdrawal.

561. Mr. Johnson notified Coinbase of the unauthorized transactions in his account.

562. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Johnson has been



damaged by the loss of over \$100,000 worth of cryptocurrency from his Coinbase Wallet Accounts.

### **Mr. Singh's Coinbase Wallet Account**

563. Mr. Singh held cryptocurrency in a Coinbase Wallet Account, including Ethereum and the stablecoin Tether (USDT).

564. On or about August 19, 2022, while in the Coinbase Wallet application, Mr. Singh interacted with a decentralized application (dapp) at the address “yield-farming.pro.” Mr. Singh unknowingly entered into a “smart contract” that allowed the dapp to withdraw and irrevocably keep cryptocurrency from Mr. Singh's Coinbase Wallet Account without his authorization.

565. Mr. Singh contacted Coinbase Support to report the loss of control of cryptocurrency in his Coinbase Wallet Account and the unauthorized transactions in his account.

566. On September 20, 2022, Mr. Singh urged Coinbase to block the dapp and flag it as malicious, which Coinbase still had not done despite Mr. Singh notifying Coinbase much earlier about the problem.

567. Mr. Singh submitted a Formal Complaint to Coinbase on September 16, 2022. Coinbase eventually denied Mr. Singh's Formal Complaint.

568. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Mr. Singh has been damaged by losing approximately \$25,000 of cryptocurrency from his Coinbase Wallet Account.

### **Ms. Tang's Coinbase Wallet Account**

569. Ms. Tang had a Coinbase Wallet Account.

570. In July and August 2022, Ms. Tang believed she was safely holding within her Coinbase Wallet account. She carefully safeguarded the credentials for her Coinbase Wallet. However, a web3 site in the Coinbase Wallet took control over Ms. Tang's Wallet without her permission. Through a "smart contract," Ms. Tang's Coinbase Wallet was completely drained of approximately \$286,000 worth of cryptocurrency in July and August 2022.

571. Ms. Tang contacted Coinbase and asked that the USDT (Tether "stablecoin") taken from her Coinbase Wallet be refunded. Coinbase refused to refund Ms. Tang for the unauthorized transactions.

572. In response to Ms. Tang's request for assistance, stated, in part, that the so-called "smart contract" that had taken control of Ms. Tang's Coinbase Wallet without warning was "a common method through which a malicious third party can target and victimize users."

573. Coinbase has refused to reverse, refund, or credit the account for the unauthorized transactions. As a result of Coinbase's conduct, Ms. Tang has been damaged by the loss of her cryptocurrency.

### **CLASS ACTION ALLEGATIONS**

574. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following class (collectively, the "Class"):

All current and former users who had funds or cryptocurrency stored on one of Coinbase's platforms, including Coinbase's exchange platforms and "Coinbase Wallet," and who subsequently lost or were deprived of access to the funds and/or cryptocurrency in their Coinbase account or "Coinbase Wallet."

575. The following individuals and entities are excluded from the proposed Class:

Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

576. Additionally, Plaintiffs Houzenga, Gambell, Johnson, Singh, Tang, and Dallalnejad are members of and seek to represent a Wallet User Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and/or (b)(3), defined as:

All current and former users of the Coinbase Wallet who had funds or cryptocurrency taken from their Coinbase Wallet by a decentralized application or “smart contract” executing a withdrawal without the user’s authorization.

577. The Georgia Plaintiffs are members of and seek to represent a Georgia Sub-Class, pursuant to Fed. R. Civ. P. 23(b)(2) and/or (b)(3), defined as:

All Georgia Residents who are current or former users of Coinbase’s platforms, including Coinbase’s exchange platform, “Coinbase Wallet,” who had funds or cryptocurrency in a Coinbase account, and who subsequently lost funds and/or cryptocurrency or were deprived of access to funds and/or cryptocurrency that had been stored in their Coinbase account or “Wallet.”

578. Plaintiffs reserve the right to modify the proposed class definitions, including but not limited to expanding the class to protect additional individuals and to assert additional sub-classes as warranted by further investigation.

579. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

580. Plaintiffs have no interests antagonistic to those of the Class.

581. **Numerosity:** There are over 100 million Coinbase users. The proposed Class and Wallet User Sub-Class are believed to be so numerous that joinder of all

members is impracticable. Upon information and belief, the total number of Class Members is in the tens of thousands, if not millions of individuals. Membership in the Class and Wallet User Sub-Class will be determined by analysis of Defendants' records.

582. **Typicality:** Plaintiffs' claims are typical of the claims of the Class and Wallet User Sub-Class. All such claims arise out of the same lax account policies, defects in the Coinbase Wallet, practices, procedures, and other actions by Defendants. The same or similar documents are used by Defendants in their dealings with Plaintiffs and Class Members. Plaintiffs and all members of the Class and Wallet User Sub-Class were injured through Defendants' uniform misconduct, negligence, and breaches of duty.

583. **Adequacy:** Plaintiffs are adequate representatives of the Class and Wallet User Sub-Class because their interests do not conflict with the interests of the Class and Wallet User Sub-Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class and Wallet User Sub-Class will be fairly and adequately protected by Plaintiffs and their counsel.

584. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs, the Class, and the Wallet User Sub-Class. The injury suffered by each individual Class and Wallet User Sub-Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for individual members of the Class to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation or even individual arbitration, the court system could not. Individualized litigation and/or arbitration presents a potential for wholly inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single forum.

585. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs, the other members of the Class, and members of the Wallet User Sub-Class. Those questions predominate over any questions that may affect individual members of the Class and Wallet User Sub-Class. Those common questions of law and fact include, without limitation:

- a. Whether Defendants owed duties to Plaintiffs and the Class, the scope of those duties, and whether Defendants breached those duties;
- b. Whether Defendants' conduct was unfair or unlawful;
- c. Whether Defendants engaged in deceptive conduct;
- d. Whether Defendants engaged in the wrongful conduct alleged herein;
- e. Whether the Electronic Funds Transfer Act ("EFTA") and Regulation E apply to Defendants;
- f. Whether Defendants violated the EFTA and Regulation E;
- g. Whether Coinbase fails to employ adequate safety and cybersecurity measures for its clients;
- h. Whether the purported "User Agreement" and its delegation clause are illegal, unconscionable, or otherwise unenforceable;
- i. Whether Coinbase's customer support system is farcical and lacking adequate ability to service Coinbase customers;
- j. Whether Defendants have been unjustly enriched as a result of their conduct of locking out Plaintiffs and the Class from their Coinbase accounts;
- k. Whether Defendants were aware of and failed to adequately respond to security issues, including failing to diligently investigate issues and expediently notify affected individuals in, and whether this caused damages to Plaintiffs and the Class;
- l. Whether the Coinbase Wallet's security is defective;
- m. Whether Plaintiffs and the Class suffered injuries from Defendants' security breaches;

- n. Whether declaratory and injunctive relief are appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class members and the public; and
- o. Whether Plaintiffs and the Class are entitled to actual damages, punitive damages, treble damages, equitable relief, and other relief as a result of Defendants' wrongful conduct.

586. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final declaratory and injunctive relief appropriate with respect to the Class in its entirety. Defendants' policies challenged herein and defects in Defendants' platforms apply to and affect Class Members and Wallet User Sub-Class Members uniformly. Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to the Plaintiffs.

587. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the accounts of Class Members, continue in their failure to give Class Members proper access to their accounts and assets, continue in their sham dispute resolution process, continue to profit from unauthorized transactions, and continue to act unlawfully as set forth in this Complaint.



**CLAIMS FOR RELIEF ON BEHALF OF THE CLASS AND  
WALLET USER SUB-CLASS**

**FIRST CAUSE OF ACTION  
(Declaratory Judgement as to Invalidity of Arbitration Provision and  
Delegation Clause and Injunctive Relief)**

588. Plaintiffs incorporate by reference and reallege paragraphs 1 to 587 contained above, as though fully set forth herein.

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

590. An actual controversy has arisen regarding Defendants' duties to its users and whether Defendants are taking adequate measures to provide Plaintiffs and Class Members with secure access to their accounts, funds, and/or cryptocurrency. An actual controversy has also arisen regarding Defendants' unconscionable User Agreement(s).

591. Coinbase has attempted to immunize itself from liability for its wrongful conduct by burying in a lengthy (and ever-changing) User Agreement a number of unconscionable provisions, including: a purported arbitration agreement

(with a sham dispute resolution process), class action waiver, and a clause purporting to exculpate Coinbase for all liability for its own negligence.

592. Coinbase's purported arbitration agreement, including the delegation clause, and class action waiver are unenforceable because they violate public policy and are both procedurally and substantively unconscionable.

593. Specifically, both the arbitration clause and its delegation clause in the User Agreement lack mutuality and impose an unfair burden on Plaintiffs that qualifies as unconscionable.

594. The User Agreement includes pretextual and unduly onerous preconditions to arbitration.

595. Coinbase's complaint process is ineffective, unavailing, and one-sided; it requires users to jump through antecedent hoops not applicable to Coinbase before initiating arbitration.

596. At least one court has already determined that both the arbitration clause and its delegation clause in Coinbase's Terms of Service are unconscionable and unenforceable. *See Bielski v. Coinbase, Inc.*, 2022 WL 1062049 (N.D. Ca. April 8, 2022).

597. A judicial declaration is necessary and appropriate so the parties may ascertain their rights, duties, and obligations with respect to these provisions.

598. The Court may use its equitable powers to declare the arbitration clause and class action waiver in Coinbase's User Agreement to be unenforceable.

599. In addition, the Court may enter a public injunction ordering Coinbase to prominently disclose to the public, in compliance with the EFTA and applicable law, Coinbase's policies for unauthorized transactions.

600. Accordingly, Plaintiffs and the Class are entitled to a declaration that the arbitration clause, including the delegation clause and dispute resolution notice provisions, in the Coinbase User Agreement (if such User Agreement is found to exist) are unconscionable and unenforceable as to Plaintiffs and as to the Class.

**SECOND CAUSE OF ACTION  
(Breach of Fiduciary Duty)**

601. Plaintiffs incorporate by reference and reallege paragraphs 1 to 587 contained above, as though fully set forth herein.

602. As the custodian of their cryptocurrency assets and acting as an agent transacting on their behalf when they wish to buy, sell, or convert crypto assets on the Coinbase platform, Coinbase has a fiduciary relationship with Plaintiffs and Class Members, and must exercise the fiduciary duties it therefore owes with the utmost good faith, integrity, and in the best interest of Plaintiffs and Class Members.

603. As discussed herein, Coinbase represents and agrees that it will act as the custodian of all funds and digital currency assets it holds in its customer accounts,

that Coinbase will securely store these funds and cryptocurrency assets, that Coinbase will hold these funds and cryptocurrency assets for the benefit of Plaintiffs and Class Members, that Coinbase will allow Plaintiffs and Class Members to control, access and withdraw their funds and cryptocurrency assets at any time, and that Coinbase will not sell, transfer, loan, hypothecate, or otherwise alienate customer cryptocurrency assets except as instructed by the customer.

604. As the custodian of their valuable assets, Plaintiffs and Class Members entrust Coinbase to ensure the safekeeping of their assets and to provide them with access to and control over their accounts and the assets within those accounts when they want.

605. Defendants owe a fiduciary duty to Plaintiffs and Class Members to provide them with immediate access to their accounts, the funds and cryptocurrency assets within those accounts, and to process only the respective customer's transactions within those accounts.

606. Defendants owe a fiduciary duty to Plaintiffs and Class Members to protect their accounts, their transactions relating to those accounts, and their funds and cryptocurrency assets within those accounts.

607. Defendants owe a fiduciary duty to Plaintiffs and Class Members to timely respond to and resolve their complaints regarding security threats, hacking,

and technological issues that preclude Plaintiffs' and Class Members' access to their accounts, account transactions, account funds, and cryptocurrency assets.

608. Defendants owe a fiduciary duty to timely notify Plaintiffs and Class Members of any security threats, hacking, and technological issues that preclude Plaintiffs' and Class Members' access to their accounts, account transactions and account funds and cryptocurrency assets.

609. Defendants breached their fiduciary duty owed to Plaintiffs and Class Members to protect their accounts, their transactions relating to those accounts, and their funds and cryptocurrency assets within those accounts.

610. Defendants breached their fiduciary duty owed to Plaintiffs and Class Members to timely respond to and resolve their complaints regarding security threats, hacking, and technological issues that preclude Plaintiffs' and Class Members' access to their accounts, account transactions and account funds and cryptocurrency assets.

611. Defendants breached their fiduciary duty owed to timely notify Plaintiffs and Class Members of any security threats, hacking, and technological issues that preclude Plaintiffs' and Class Members' access to their accounts, account transactions, account funds, and cryptocurrency assets.

612. Defendants breached their fiduciary duty owed to properly employ standard measures to verify the identity of users, including Plaintiffs and Class Members, to reduce the risk of security threats, hacking, and technological issues that led to Plaintiffs' and Class Members' loss of assets and loss of access to their accounts.

613. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by, among other things, processing transactions within Plaintiffs' and Class Members' accounts when not initiated by Plaintiffs and Class Members, causing unreasonable delays in allowing Plaintiffs and Class Members to access their accounts or barring account access for unreasonably long periods of time, and/or refusing to return Plaintiffs' and Class Members' funds.

614. Defendants also breached their fiduciary duties owed to Plaintiffs and Class Members by failing to act with utmost good faith and in the best interests of Plaintiffs and Class Members by, among other things, ignoring or failing to timely respond to and resolve Plaintiffs' and Class Members' repeated complaints and other communications demanding access to their Coinbase accounts.

615. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have been damaged in an amount to be proven at trial, including nominal damages.

616. In addition to actual or consequential damages, Plaintiffs and Class Members are entitled to pre-judgment interest, attorney's fees and costs, along with any relief that this Court deems just and proper.

**THIRD CAUSE OF ACTION**  
**(Breach of Contract and the Implied Covenant of**  
**Good Faith and Fair Dealing)**

617. Plaintiffs incorporate by reference and realleges paragraphs 1 to 587 contained above, as though fully set forth herein.

618. Plaintiffs and Class Members each entered into a written contract, the User Agreement, with Defendants upon their registration for a Coinbase account. Plaintiffs and Class Members were presented with the User Agreement on a take-it-or-leave it basis and had no opportunity to negotiate any of the specific terms or provisions thereunder.

619. Every contract, including the User Agreement, contains an implied duty of good faith and fair dealing. Defendants entered into and are bound by the User Agreements with Plaintiffs and Class Members, which are valid and enforceable contracts that contain an implied duty of good faith and fair dealing.

620. Defendants breached the User Agreement and the implied covenant of good faith and fair dealing by, among other things, failing to discharge their obligations and provide the services they promised in exchange for the transaction

fees they charged Plaintiffs and Class Members for each transaction in their account and for the monies they earned on the funds within Plaintiffs' and Class Members' accounts.

621. Defendants breached the User Agreement and the implied covenant of good faith and fair dealing by failing to protect Plaintiffs' and Class Members' accounts, their transactions relating to those accounts, and their funds and cryptocurrency assets within those accounts.

622. Defendants breached the User Agreement and the implied covenant of good faith and fair dealing by failing to timely respond to and resolve Plaintiffs' and Class Members' complaints regarding security threats, hacking, and technological issues that precluded Plaintiffs and Class Members' access to their accounts, account transactions, account funds, and cryptocurrency assets.

623. Defendants breached the User Agreement and the implied covenant of good faith and fair dealing by failing to return Plaintiffs' and Class Members' account funds and cryptocurrency assets.

624. As a result of Defendants' breach of their contractual duties, obligations and/or promises arising under the User Agreement and the implied covenant of good faith and fair dealing, Plaintiffs and Class Members were damaged by, including but not limited to, their payment of transaction fees, the loss of use of their accounts, the



inability to access the funds and cryptocurrency assets in their accounts and the loss of value of those assets, all in an amount to be proven at trial.

625. In addition to Plaintiffs' and Class Members' actual contract damages, Plaintiffs and Class Members seek recovery of their attorney's fees, costs to the extent provided by the User Agreement and pre-judgment interest.

**FOURTH CAUSE OF ACTION  
(Unjust Enrichment)**

626. Plaintiffs incorporate by reference and reallege paragraphs 1 to 587 contained above, as though fully set forth herein.

627. Plaintiffs and Class Members conferred a benefit upon Defendants by depositing their currency funds and cryptocurrency assets into their accounts maintained by Defendants and maintained such assets in those accounts, which enabled Defendants to profit from the investment and trading of such assets.

628. Plaintiffs and Class Members conferred a benefit upon Defendants by paying fees to Defendants in order to conduct transactions in their accounts, maintain their accounts, and have access to those accounts.

629. Coinbase collected transaction fees from unauthorized transactions, including cryptocurrency conversions and transfers, in the accounts of Plaintiffs and Class Members.

630. As a result of Defendants' actions and omissions alleged herein, Defendants have been unjustly enriched at the expense of Plaintiffs and Class Members. Under principles of equity and good conscience, Defendants should not be permitted to retain the transaction fees paid by Plaintiffs and Class Members or the assets held within Plaintiffs' and Class Members' accounts.

631. Plaintiffs and Class Members are entitled to restitution of, disgorgement of, and/or the imposition of a constructive trust upon all fee revenue, income, profits, and other benefits obtained by Defendants at the expense of Plaintiffs and Class Members resulting from Defendants' actions and/or omissions alleged herein, all in an amount to be proven at trial. Plaintiffs and Class Members also are entitled to attorney's fees, costs and prejudgment interest, along with any relief that this Court deems just and proper.

632. Plaintiffs and the Class have no adequate remedy at law.

**FIFTH CAUSE OF ACTION**  
**(Violations of the Electronic Funds Transfer Act and Regulation E)**

633. Plaintiffs incorporate by reference and reallege paragraphs 1 to 587 contained above, as though fully set forth herein.

634. Congress created the Electronic Funds Transfers Act ("EFTA"), 15 U.S.C. § 1693, et seq., in order to establish a framework to regulate electronic fund

and remittance transfer systems, and to establish individual consumer rights related to electronic fund transfers.

635. Regulation E is promulgated pursuant to the EFTA. It governs how financial institutions must provide information and investigate an unauthorized electronic fund transfer. *See, e.g.*, 12 C.F.R. § 1005.11; 12 C.F.R. 205.11.

636. The EFTA provides, in relevant part: if a financial institution receives notice (or constructive notice) of an error (e.g. an unauthorized electronic fund transfer) within sixty days of sending a consumer notice of an electronic funds transfer, that financial institution must timely investigate the alleged error and timely report to the consumer the results of its investigation and determination as to whether an error occurred. *See* 15 U.S.C. § 1693f(a); 12 C.F.R § 205.11; 12 C.F.R. Pt. 205, Supp. I.

637. “If the financial institution determines that an error did occur, it shall promptly, but in no event more than one business day after such determination, correct the error, subject to section 1693g of this title, including the crediting of interest where applicable.” 15 U.S.C. § 1693f(b).

638. In an action under 15 U.S.C. § 1693(b), a financial institution may be subject to treble damages if the court finds that:

- (1) the financial institution did not provisionally recredit a consumer's account within the ten-day period specified in

subsection (c), and the financial institution (A) did not make a good faith investigation of the alleged error, or (B) did not have a reasonable basis for believing that the consumer's account was not in error; or

(2) the financial institution knowingly and willfully concluded that the consumer's account was not in error when such conclusion could not reasonably have been drawn from the evidence available to the financial institution at the time of its investigation[.]

15 U.S.C. § 1693f(e).

639. Defendants are financial institutions as defined by the EFTA because they directly or indirectly hold consumers' accounts, namely Plaintiffs and Class Members' accounts.

640. Plaintiffs and Class Members' Coinbase accounts are "accounts" as defined by the EFTA because they are checking, savings, or other consumer asset accounts held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes.

641. Plaintiffs and Class Members are consumers under the EFTA.

642. Plaintiffs and Class Members provided timely actual and/or constructive notice to Defendants of unauthorized transfers from their Coinbase accounts.

643. Defendants failed to conduct a timely investigation of Plaintiffs and Class Members' accounts that complied with the EFTA and Regulation E.

644. Coinbase failed to correct the errors, i.e., the unauthorized electronic fund transfers, in Plaintiffs' and Class Members' accounts by timely crediting (and/or provisionally crediting) their accounts for the amount drained.

645. Given the telltale signs of suspicious activity and theft from Plaintiffs' accounts (and indeed from numerous other users of Coinbase's platform), Coinbase could not reasonably have concluded the unauthorized transactions in Plaintiffs' Coinbase accounts were not in "error."

646. In violation of 15 U.S. C. § 1693f(e), Coinbase wrongfully, knowingly, and willfully concluded that the unauthorized transfers from Plaintiffs and Class Members' Coinbase accounts were not in error.

647. Because Coinbase never provided disclosures to Plaintiffs and Members that were compliant with 12 C.F.R. § 1005.7(b), Plaintiffs and Class Members have no liability for the unauthorized electronic fund transfers under 15 U.S.C. § 1693g and/or 12 C.F.R. § 1005.6.

648. As a result of Coinbase's failures to comply with the EFTA and regulations thereunder, Plaintiffs and the Class Members were injured.

649. Accordingly, pursuant to 15 U.S.C § 1693f and 15 U.S.C. § 1693m, Plaintiffs and Class Members are entitled to compensatory damages, treble damages, attorneys' fees, costs of the action, and/or statutory damages.

**SIXTH CAUSE OF ACTION**  
**(Violation of EFTA and Regulation E Customer Service Provisions,**  
**15 U.S.C. § 1693f(f)(6); 12 C.F.R. § 1005.11(a)(vii))**

650. Plaintiffs incorporate by reference the allegations in paragraphs 1 through 587 contained above, as though fully set forth herein.

651. The EFTA, 15 U.S.C. § 1693f(f)(6) and Regulation E, 12 C.F.R. § 1005.11(a)(7) require financial institutions to address “a consumer’s request for additional information or clarification concerning an electronic fund transfer.”

652. Defendants violated the EFTA and Regulation E by failing to timely provide information or clarification concerning an electronic fund transfer, including requests Plaintiffs and the Class made to determine whether there were unauthorized electronic transfers from their accounts. *See* 15 U.S.C. § 1693f(f)(6); 12 C.F.R. § 1005.11(vii).

653. Accordingly, Defendants are liable to Plaintiffs and the Class for statutory damages, attorneys’ fees, and costs for this claim pursuant to 15 U.S.C § 1693m.

**SEVENTH CAUSE OF ACTION**  
**(Negligence)**

654. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

655. At all times herein relevant, Defendants owed Plaintiffs and Class Members as a duty of care, *inter alia*, to act with reasonable care to secure and safeguard assets held in their Coinbase accounts and to safeguard the sensitive information stored in those accounts, including by establishing and maintaining measures that comply with highest standards of cryptocurrency, standards for money transmitters and financial institutions, laws, regulations, and Coinbase's own internal policies. Defendants undertook this obligation and assumed these responsibilities upon accepting Plaintiffs' and Class Members' cryptocurrency and funds, such as cryptocurrency, on its platform.

656. Coinbase held itself out to be a highly secure platform for holding cryptocurrency and in full compliance with the stringent requirements of state and federal authorities.

657. As more fully set forth above, Coinbase's negligent actions include:

- a. Failing to implement and monitor adequate cybersecurity measures to protect its users against rampant hacking and theft on its platform;
- b. Failing to detect suspicious activity in Plaintiffs' accounts;
- c. Authenticating new devices never before used;

- d. Authenticating access to accounts from locations far away from the user's usual and actual location;
- e. Failing to provide adequate customer support services to remedy ordinary account problems and unauthorized account access;
- f. Approving the unauthorized complete depletion of accounts;
- g. Failing to timely detect and mitigate suspicious activity in and subsequent theft from Plaintiffs' account; and
- h. Failure to insure or recover Plaintiffs' losses.

658. Defendants breached their duty to Plaintiffs and Class Members by providing cryptocurrency custody services that failed to meet the applicable standard of care.

659. Defendants breached their duty to Plaintiffs and the Sub-Class by failing to protect Coinbase Wallet users from withdrawals, such as those caused by "smart contracts," that can occur without a user's authorization and/or without a user entering the Wallet's recovery phrase to approve the withdrawal.

660. Defendants breaches are so egregious they amount to gross negligence.

661. Plaintiffs and Class Members have incurred substantial financial damages as a direct result of Defendants' breach of duty of reasonable care.



662. Plaintiffs and Class Members have also incurred costs in terms of time, effort, and money expended as a result of Defendants' breach, insufficient customer support, and invalid and onerous dispute resolution process.

**EIGHTH CAUSE OF ACTION  
(Conversion)**

663. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

664. Plaintiffs and the Class deposited funds and/or cryptocurrency with Defendants.

665. Plaintiffs and the Class owned, possessed, and had a right to possess the property deposited with Defendants.

666. Defendants wrongfully refused to return the property deposited by Plaintiffs and the Class upon proper demand.

667. Defendants have refused to return, lost, or wrongfully disposed of the property deposited by Plaintiffs and the Class.

668. Plaintiffs and the Class did not consent to the misconduct described herein or to the transfer of their property to third parties.

669. Defendants' misconduct injured Plaintiffs and the Class.

**NINTH CAUSE OF ACTION  
(Bailment)**

670. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

671. Plaintiffs and the Class deposited funds and/or cryptocurrency with Coinbase.

672. Coinbase accepted delivery of the funds and/or cryptocurrency with the understanding that the funds and/or cryptocurrency be returned to Plaintiffs and the Class or delivered to another person for safekeeping on behalf of Plaintiffs and the Class.

673. Plaintiffs and the Class provided consideration for the cryptocurrencies and funds deposited with Coinbase through, for example, fees and commissions collected by Coinbase.

674. Coinbase, as the bailee of Plaintiffs' and Class Members' personal property, had an obligation to return or account for the deposited personal property upon demand.

675. By their own acts or omissions, Coinbase caused the personal property deposited by Plaintiffs and the Class to be lost.

676. Coinbase refused to return the personal property deposited by Plaintiffs and the Class.

677. Coinbase refused to provide complete disclosure to Plaintiffs and the Class regarding how the loss of their property occurred.

678. Coinbase willfully, or by gross negligence, permitted the loss of Plaintiffs' and Class Members' personal property.

679. As a result of Coinbase's failure to uphold its obligations as a bailee, including the exercise of proper care and diligence to protect the property bailed, Plaintiffs and the Class have been deprived of their personal property and injured.

**TENTH CAUSE OF ACTION  
(Violation of California Uniform Commercial Code Division 8,  
Cal. Com. Code § 8507(b))**

680. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

681. Coinbase has held itself out as a "securities intermediary" with respect to assets in a Coinbase account or Coinbase wallet.

682. Under Cal. Com. Code § 8102(a)(7), the owner of financial assets held in an account with a securities intermediary is an "entitlement holder."

683. At the time of the unauthorized transfers alleged herein, Plaintiffs and Class were "entitlement holders" with respect to the assets held in Plaintiffs' and Class Members' Coinbase accounts or wallets.

684. A communication to a securities intermediary directing the securities intermediary to transfer a certain financial asset is an “entitlement order.” See Cal. Com. Code § 8102(a)(8).

685. An entitlement order is only effective if it is made by the entitlement holder or an authorized agent or ratified by an appropriate person (i.e., the entitlement holder) as defined by Cal. Com. Code § 8107(b).

686. The orders for the unauthorized transfers from Plaintiffs’ and the Class Members’ Coinbase accounts were ineffective because they were not made Plaintiffs or by Plaintiffs’ authorized representatives, nor were they ratified by Plaintiffs.

687. Defendants completed the unauthorized transfers alleged herein despite the fact that they were made pursuant to ineffective entitlement orders.

688. Pursuant to Cal. Com. Code § 8507(b), Defendants are obligated to credit Plaintiffs and Class’s accounts to correct the unauthorized transfers and to pay or credit any payments or distributions that Plaintiffs and Class did not receive as a result of the wrongful transfers, in addition to liability for damages.

689. Plaintiffs and the Class were injured as a direct and foreseeable consequence of Defendants’ transfers of Plaintiffs and the Class Members’ financial assets pursuant to invalid entitlement orders and Defendants’ failure to credit Plaintiffs’ and Class Members’ accounts to correct the unauthorized transfers.

**ELEVENTH CAUSE OF ACTION**  
**(Violation of Consumer Legal Remedies Act**  
**Cal. Civ. Code §§ 1750, *et seq.*)**

690. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

691. The Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (“CLRA”) is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property, or services to consumers primarily for personal, family, or household use.

692. Coinbase and Coinbase Global are each a “person” as defined by Civil Code §§ 1761(c) and 1770. Coinbase provided “services” as defined by Civil Code §§ 1761(b) and 1770.

693. Plaintiffs and the Class are and at all relevant times have been “consumers” under the terms of the California Consumer Legal Remedies Act (“CLRA”) at all relevant times because they were individuals seeking or acquiring, by purchase or lease, goods or services for personal, family, or household purposes.

694. Coinbase engaged in deceptive and unconscionable trade practices that violated the CLRA, including:

- a. Misrepresenting the standard, quality, or grade of Coinbase’s services;

- b. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not; and
- c. Inserting an unconscionable provision in a contract.

695. Coinbase engaged in unfair and deceptive acts or practices in violation of Cal. Civ. Code §§ 1770(a), including, among other things: (a) improperly and unreasonably preventing Plaintiffs and the Class from accessing their accounts and funds, either for extended periods of time or permanently; (b) failing to timely respond to requests for support; (c) failing to safeguard customer funds with the advertised “bank-level” and high security measures; (d) not compensating the Plaintiffs and the Class for Defendants’ wrongdoing and their losses; and (e) misleading consumers about the security of assets entrusted to Coinbase.

696. Coinbase’s misrepresentations were material. Coinbase’s violations of the CLRA were a substantial factor in causing Plaintiffs and the Class to use Coinbase’s services.

697. As a direct and proximate consequence of the actions described above, Plaintiffs and the Class suffered injuries.

698. Coinbase’s conduct described herein was malicious, fraudulent, and wanton. Coinbase intentionally and knowingly provided misleading information to Plaintiffs and the Class and refused to remedy breaches of its systems long after

learning of the inadequacy of its security measures and widespread unauthorized access of Coinbase accounts.

699. Coinbase’s misrepresentations regarding its services and its inclusion of unconscionable provisions in the User Agreement are ongoing. Unless enjoined by the Court, the conduct complained of will continue to deceive and cause injury to the general public.

**TWELFTH CAUSE OF ACTION  
(Violation of California False Advertising Law,  
Cal. Bus. & Prof. Code §§ 17500 *et seq.*)**

700. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

701. Coinbase violated California False Advertising Law, Cal. Bus & Prof. Code §§ 17500 *et seq.* (“FAL”) by seeking to induce consumers, including Plaintiffs and the Class, to do business with Defendants by marketing its services with false and misleading statements concerning the services.

702. Coinbase’s misrepresentations were material. Defendants’ violations of the FAL were a substantial factor in causing Plaintiffs and the Class to use Coinbase’s services.

703. As a direct and proximate consequence of the actions described above, Plaintiffs and the Class suffered injuries.

704. Coinbase’s conduct described herein was malicious, fraudulent, and wanton. Coinbase intentionally and knowingly provided misleading information to Plaintiffs and the Class and refused to remedy breaches of its systems long after learning of the inadequacy of its security measures and widespread unauthorized access of Coinbase accounts.

705. Coinbase’s misrepresentations regarding its services and its inclusion of unconscionable provisions in the User Agreement are ongoing and, unless enjoined by the Court, will continue to deceive and cause injury to the general public.

**THIRTEENTH CAUSE OF ACTION  
(Violation of Unfair Competition Law,  
Cal. Bus. & Prof. Code §§ 17200 *et seq.*)**

706. Plaintiffs incorporate by reference the allegations in paragraphs 1 to 587 above as though fully set forth herein.

707. Plaintiffs, Coinbase, and Coinbase Global are each a “person” as defined by Cal. Bus. & Prof. Code § 17201.

708. The California Unfair Competition Law (“California UCL”), Cal. Bus. & Prof. Code § 17200, defines “unfair competition” as “any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.”



709. Under the California UCL, a business act or practices is “unfair” if the defendant’s conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing such acts or practices are outweighed by the gravity of harm Plaintiffs incurred.

710. Coinbase and Coinbase Global Inc. engaged in unfair and deceptive acts or practices in violation of the California UCL, including among other things: (a) improperly and unreasonably preventing Plaintiffs and the Class from accessing their accounts and funds, either for extended periods of time or permanently; (b) failing to timely respond to requests for support; (c) failing to safeguard customer funds with the advertised “bank-level” and high security measures; (d) not compensating the Plaintiffs and the Class for Defendants’ wrongdoing and their losses; and (e) misleading consumers about the security of assets entrusted to Coinbase.

711. Moreover, Coinbase engaged in unlawful acts or practices in violation of the California UCL through noncompliance with laws regulating the transfer of funds, including the Electronic Fund Transfers Act and Regulation E.

712. Plaintiffs have been deceived as a result of their reliance of Defendants' material representations and omissions, which are described above and would be considered important to any reasonable consumer.

713. Defendants knew, or should have known, its material misrepresentations and omissions would be likely to deceive and harm California Plaintiffs and the general public.

714. Defendants received proper notice of their alleged violations of the California UCL via Plaintiffs' complaints to Coinbase, in addition to the original complaint filed in this action. Plaintiffs found the responses to their notices to Coinbase to be unsatisfactory.

715. Defendants' conduct is substantially injurious to consumers, offends legislatively declared public policy, is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described conduct.

716. As a direct and proximate result of Defendants' unfair or deceptive acts or practices, California Plaintiffs and Subclass Members suffered and will continue to suffer actual damages in that they have lost assets entrusted to Coinbase and

wasted time in Coinbase’s cumbersome, unfair, and futile complaint process, in addition to injuries suffered as a result of Defendants’ acts or practices in failing to reverse or refund funds in compliance with Regulation E and the Electronic Funds Transfer Act.

717. Defendants’ violations present a continuing risk to the California Plaintiffs and to the general public. Defendants’ unlawful acts and practices affect the public interest.

718. California Plaintiffs and Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief under Cal. Bus. & Prof. Code § 17203, reasonable attorney’s fees and costs, and any other relief that is just and proper.

**CLAIM FOR RELIEF ON BEHALF OF THE GEORGIA SUBCLASSES**

**FOURTEENTH CAUSE OF ACTION**  
***On Behalf of the Georgia Plaintiffs and Georgia Subclass***  
**(Deceptive Practice – O.C.G.A. § 10-1-393)**

719. The Georgia Plaintiffs incorporate by reference and reallege paragraphs 1 to 587 contained above, as though fully set forth herein.

720. Coinbase Global and Coinbase Inc. are each a “person” as defined by the Georgia Fair Business Practices Act (“Georgia FBPA”). O.C.G.A. § 10-1-392(a)(24).

721. Georgia Plaintiffs and Georgia Subclass are “consumers” within the meaning of the Georgia FBPA. O.C.G.A. § 10-1-392(a)(6).

722. The opening of an account and placing assets with Coinbase by the Georgia Plaintiffs and Georgia Subclass constituted “consumer transactions” as defined by the Georgia FBPA. O.C.G.A. § 10-1-392(a)(10).

723. The Georgia FBPA declares “[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce” to be unlawful, O.C.G.A. § 10-1-393(a), including but not limited to “representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, or benefits that they do not have,” “[r]epresenting that goods or services are of a particular standard, quality, or grade ... if they are of another,” and “[a]dvertising goods or services with intent not to sell them as advertised,” *id.* §§ 10-1-393(b)(5), (7) & (9).

724. Defendants’ acts and practices as alleged herein also constitute “unfair” and “deceptive” acts and practices within the meaning of the Georgia FBPA. In the course of conducting business, Defendants have violated the Georgia FBPA’s proscription against unfair business practices by, among other things: (a) improperly and unreasonably preventing the Georgia Plaintiffs and the Georgia Subclass from accessing their accounts and funds, either for extended periods of time or

permanently; (b) failing to timely respond to requests for support; (c) failing to safeguard customer funds with the advertised “bank-level” and high security measures; (d) not compensating the Georgia Plaintiffs and the Georgia Subclass for Defendants’ wrongdoing and their losses; and (e) misleading consumers about the security of assets entrusted to Coinbase.

725. Defendants’ unfair business conduct is substantially injurious to consumers, offends legislatively-declared public policy as announced by the violations of the laws alleged, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendants’ wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants’ legitimate business interests other than engaging in the above-described wrongful conduct.

726. The Georgia Plaintiffs, in fact, have been deceived as a result of their reliance of Defendants’ material representations and omissions, which are described above and would be considered important to any reasonable consumer.

727. As a direct and proximate result of Defendants’ unfair or deceptive acts or practices, Plaintiffs and Class Members suffered and will continue to suffer actual damages in that they have lost assets entrusted to Coinbase and wasted time in

Coinbase's cumbersome, unfair, and futile complaint process, among other damages.

728. Defendants' violations present a continuing risk to the Georgia Plaintiffs and to the general public. Defendants' unlawful acts and practices affect the public interest.

729. The Georgia Plaintiffs and Class Members are entitled to equitable relief.

730. Defendants received proper notice of their alleged violations of the Georgia FBPA via Plaintiffs' written complaints to Coinbase, in addition to the original complaint filed in this action. The Georgia Plaintiffs found the responses to their notices to Coinbase to be unsatisfactory.

731. Thus, pursuant to O.C.G.A. § 10-1-399, the Georgia Plaintiffs seek, in addition to equitable relief, actual and statutory damages, attorneys' fees and expenses, treble damages, and punitive damages as permitted under the Georgia FBPA and applicable law.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendants as follows:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class and Sub-Class as requested herein;
- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order for declaratory and injunctive relief, including public injunctive relief, and for money damages under Federal Rules of Civil Procedure Rule 23, appointing Plaintiffs as Class Representatives, and appointing their attorneys as Class Counsel;
- d. A judgment for actual damages;
- e. A judgment for compensatory damages;
- f. A judgment for disgorgement of transaction fees, income, and other profits;
- g. A judgment for injunctive relief enjoining Defendants from engaging in future unlawful activities complained of herein, including violations of the federal and state laws raised in the Complaint;

- h. An injunction ordering that Defendants shall engage in proactive monitoring of account takeovers and other corrective actions so that customer accounts, funds, and cryptocurrency can be accessed without unreasonable delay;
- i. An order directing Coinbase to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable cybersecurity laws and regulations and to protect Coinbase users and account holders from a repeat of the damaging events described herein, including, but not limited to, putting forward for stockholder vote, resolutions for amendments to the Company's Bylaws or Articles of Incorporation and taking such other action as may be necessary to place before stockholders for a vote of the following corporate governance policies:
  - i. a proposal to enhance security and cybersecurity around data privacy and system security;
  - ii. a proposal to strengthen the Company's controls over accounting and financial reporting;
  - iii. a proposal to strengthen Board oversight and supervision of Coinbase's safety, cybersecurity and customer services practices;
  - iv. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater stockholder input into the policies and guidelines of the Board;
  - v. a proposal to appoint at least two additional independent



board members with established reputations in cybersecurity and with substantial experience in governance, risk, compliance and particularly cybersecurity issues;

- vi. a proposal to enhance and/or augment the audit, risk and compliance committees of the Board to oversee internal controls and compliance processes;
  - vii. a proposal to ensure that the Chief Information Security Officer (CISO); Chief Compliance (CCO); Chief Risk Officer (CRO); Chief Legal Officer(s) (CLO); and other company leadership have (1) necessary subject matter and regulatory expertise; (2) direct reporting authority to the Board; and (3) adequate autonomy and resources to carry out their responsibilities;
  - viii. a proposal to review and implement revised codes of conduct, policies and procedures, training, integrity hotlines, auditing and monitoring processes and procedures;
  - ix. a proposal to review and implement policies and procedures for escalating internal cybersecurity and regulatory issues internally and to the Board; and
  - x. a proposal to review and implement the confidential reporting structure and investigative process of complaints within the company;
- j. An accounting of all amounts that Defendants unjustly received, retained, and/or collected as a result of their unlawful acts and omissions;
- k. A judgment for exemplary and punitive damages for Defendants' knowing, willful, and/or intentional conduct;
- l. Pre-judgment and post-judgment interest;

- m. A judgment for reasonable attorney fees and costs of this suit, pursuant to O.C.G.A. § 13-6-11 due to Defendants' bad faith and stubborn litigiousness, O.C.G.A. § 10-1-393, the EFTA, and other applicable statutes;
- n. A judgment for all such other and further relief as the Court deems equitable, up to and including appointment of a corporate monitor to oversee cybersecurity enhancements.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury on all issues so triable.

DATED: October 21, 2022

HERMAN JONES LLP

By: /s/ John C. Herman

John C. Herman

Ga. Bar No. 348370

Candace N. Smith

Ga. Bar No. 654910

Steven A. Vickery

Ga. Bar No. 816854

3424 Peachtree Road, N.E., Suite 1650

Atlanta, Georgia 30326

Telephone: (404) 504-6500

Facsimile: (404) 504-6501

jherman@hermanjones.com

csmith@hermanjones.com

svickery@hermanjones.com

Serina M. Vash

(NJ Bar. No. 041142009)

(admitted *pro hac vice*)

HERMAN JONES LLP

153 Central Avenue #131

Westfield, New Jersey 07090

Tel.: (404) 504-6516

Fax: (404) 504-6501

svash@hermanjones.com

*Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I hereby certify that I have this day electronically filed this document with the Clerk of the District Court, and the CM/ECF system will send notification of such filing to all attorneys of record.

Dated: October 21, 2022

/s/ John C. Herman  
John C. Herman  
*Counsel for Plaintiffs*