UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IRA FINANCIAL TRUST,	:	
Plaintiff,	:	Case No.
-against-	:	
GEMINI TRUST COMPANY, LLC,	:	
Defendant.	:	

COMPLAINT

Plaintiff IRA Financial Trust ("***IRA***") brings this action against Defendant Gemini Trust Company, LLC ("***Gemini***") and alleges as follows:

INTRODUCTION

1. Gemini is a prominent crypto-asset exchange owned by Tyler and Cameron Winklevoss that claims to have more than $30 billion of assets under management. Gemini bills itself as "Set[ting] the standard for crypto cybersecurity." Indeed, Gemini builds its public reputation around security, claiming, for example, that, "We have operated from day one with a security-first mentality and have focused on providing our customers with layered security features to help them protect their Gemini accounts. Simply put, trust is our product."

2. Gemini boasts of supposedly industry leading security protections, such as two-factor authentication, "whitelisting" withdrawal addresses, and fraud detection algorithms. Gemini says that these protections, among others, "eliminate single points of failure."

3. *This was false*.

4. In reality, Gemini's greedy focus on lining its owners' pockets at the expense of security caused tens of millions of dollars in damages to customers and to IRA.

5. IRA is a leading provider of self-directed retirement accounts – *i.e.*, retirement accounts that allow the owner to invest in traditional and alternative investments without the restrictions that come with institutionally managed retirement accounts. IRA handles the administrative aspects of ensuring that these accounts comply with the applicable IRS regulations but never takes custody of the assets. Rather, IRA partners with third-party exchanges that serve as custodians, securing the underlying assets.

6. In 2019, IRA was one of the first providers to allow customers to purchase crypto assets directly in their retirement accounts. Because IRA never takes custody of its clients' assets, IRA needed to partner with a crypto exchange to handle trading, custody, and security of the crypto assets. This led IRA to Gemini.

7. When selecting a crypto exchange to safeguard its customers' assets, IRA focused on security. IRA selected Gemini as the exchange to secure customers' crypto assets largely because of Gemini's detailed statements about its industry-leading focus on security. Based on these statements, IRA selected Gemini, becoming an institutional customer.

8. Under IRA's arrangement with Gemini, Gemini directly onboarded all customers through Gemini's systems. The customers who elected to transact in crypto assets interacted directly with Gemini, had Gemini accounts, received crypto statements from Gemini, and could set their security preferences on the Gemini system (*e.g.*, enabling two-factor authentication). Customers even received a video welcome from the Winklevoss brothers upon signing up. Customer funds used to purchase crypto assets were sent to a Gemini bank account, and Gemini held custody of the purchased crypto assets. At no time did IRA have custody of any customer crypto assets.

9. Gemini established and maintained the security protocols used to safeguard crypto assets on its exchange, from conducting the Know Your Customer diligence during Gemini's onboarding process, to developing, deploying, monitoring, and updating the various security measures listed on its website.

10. Quickly, IRA experienced high client demand for crypto accounts. This caused problems with Gemini's systems, which could not handle onboarding customers at the speed with which they were signing up. As a result, Gemini *strongly* pressured IRA to switch from using Gemini's web-based platform to the Gemini API—Application Programming Interface—which Gemini said would streamline the process of onboarding customers. At no time did Gemini warn IRA that switching to the API would weaken the security protections over customers' crypto assets.

11. Instead, when customers expressed concerns to IRA about the security of the Gemini exchange, Gemini doubled-down by instructing IRA to tell its customers that "security events on the broader Gemini platform" were insured.

12. But unbeknownst to IRA, the Gemini API had a fatal flaw. Contrary to Gemini's many representations about security, Gemini designed its API with a single point of failure. If breached, this single point of failure allowed a bad actor to steal all crypto assets held by the customers of an institutional customer, like IRA.

13. Gemini set up the customer accounts such that IRA was the "master" account and all of Gemini's IRA customers were sub-account holders under the IRA account. As part of this system, Gemini provided IRA with a "master key." IRA has since learned—the hard way, as explained below—that whoever possesses the master key can bypass all the supposed security protections. For example, the holder of the master key can transfer and withdraw crypto assets

without getting a client's second-factor authorization. Critically, ***Gemini never informed IRA about the power of this master key***. To the contrary, Gemini itself handled IRA's master key as if it were a mundane piece of information, repeatedly exchanging unsecured, unencrypted emails with IRA containing the master key.

14. What's more, Gemini's security protocol allowed the possessor of a master key to transfer assets between sub-accounts. IRA was not aware of this functionality, nor would it have allowed it. In fact, there would never have been a legitimate reason to transfer funds between different customers' retirement accounts. Thus, not only did Gemini's system harbor a single-point-of-failure, but it also contained a sweeping vulnerability that allowed for a breach of a single customer account to give the bad actor access to all accounts. Gemini failed to warn IRA of any of this.

15. When pressuring IRA to switch to the Gemini API, Gemini focused on allowing more and more customers to onboard with Gemini, at the expense of security. Upon information and belief, Gemini made many millions of dollars in commissions from IRA customers and wanted to keep the cash flowing (IRA does not itself earn any commissions for crypto trades). Gemini prioritized revenue over security, contrary to its public proclamations.

16. Unbeknownst to IRA, hackers were able to gain control of IRA's master key by committing crimes. Once the hackers had the master key, they were able to exploit the vulnerabilities in Gemini's API to effectuate thousands of transactions within a very short period, transferring tens of millions of dollars' worth of Bitcoin and Ether belonging to hundreds of customers into a single customer retirement account, and then withdrawing all such assets.

17. ***But for Gemini's fundamentally flawed API security architecture, these losses would not have occurred***. Had Gemini's representations about security protections such as two-

factor authentication been true, the unauthorized transfers could not have been made. Nor would the transfers have been possible had there been a prohibition on transferring assets between retirement accounts – there is never a legitimate reason for one retirement account to transfer funds to another person's retirement account. Gemini knew this. Suddenly, hundreds of retirement accounts were transferring tens of millions of dollars in crypto assets to another retirement account and then withdrawing all of the assets. This fraud could not have been more obvious to Gemini. Yet Gemini permitted these transfers to occur and, contrary to its representations, did not detect them with anti-fraud systems. Amazingly, *it was IRA that had to alert Gemini*—the so-called leader in safeguarding crypto-assets—of the obvious fraud occurring on Gemini's platform.

18. It gets worse. Despite the large number of IRA customers who were trading crypto assets through Gemini, Gemini had refused to provide IRA with a phone number to use in case of an emergency. And IRA did not have the ability to freeze crypto accounts. Thus, once IRA discovered the hack, it was left to frantically email Gemini—again and again—to get all accounts frozen. Remarkably, ***it took six emails from IRA and nearly two hours for Gemini to freeze all customer accounts***. In the interim, millions of dollars in crypto assets were stolen.

19. Gemini knew about the risks attendant to crypto assets. In fact, it built its public image around purportedly mitigating those risks. But like so much else in the world of crypto, Gemini's image is just that: an image. In reality, Gemini brushes security aside when there is a chance to earn more revenue. As a result, IRA and the customers suffered tens of millions of dollars in damages that, had Gemini's representations been true, never would have occurred.

PARTIES, JURISDICTION, AND VENUE

20. IRA is a South Dakota trust company that maintains its principal place of business and "nerve center" in South Dakota. IRA's sole owner is a Florida LLC that maintains its principal place of business and "nerve center" in Florida. That entity, in turn, is owned by two Florida trusts, whose trustees and beneficiaries are all residents of and domiciled in Florida.

21. Gemini is a New York limited liability company that, upon information and belief, maintains its principal place of business and "nerve center" in New York. Upon information and belief, none of Gemini's members, or the ultimate members thereof, are citizens of, residents of, or domiciled in South Dakota or Florida for diversity purposes.

22. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332(a)(1) because the amount in controversy exceeds $75,000, exclusive of interest and costs, and IRA and Gemini are citizens of different states.

23. This Court has personal jurisdiction over Gemini, which is incorporated in New York.

24. Venue is proper in this District under 28 U.S.C. § 1391(b) because Gemini resides in this District, a substantial part of the events or omissions giving rise to the claim occurred in this District, and Gemini is subject to the Court's personal jurisdiction with respect to this action within this District.

25. This is an action for fraud, negligence, gross negligence, violations of NY GBL § 349, contribution, defamation, and tortious interference, with an amount in controversy in excess of $75,000, exclusive of fees and costs.

26. All conditions precedent to the maintenance of this action have occurred or otherwise been waived or would be futile.

27. IRA has retained undersigned counsel to represent it in this action and is required to pay counsel a reasonable fee for their services.

FACTUAL ALLEGATIONS

Background

28. IRA is a regulated South Dakota trust company that allows its customers to invest in alternative assets such as crypto assets through self-directed retirement accounts.

29. IRA charges flat administration fees (as opposed to earning commissions per transaction) and does not sell investments or offer investment advice. IRA does not take custody over any assets.

30. Gemini is a New York limited liability company that operates a cryptocurrency exchange that allows customers to buy, sell, and store digital assets. Gemini takes custody over such assets.

31. Gemini was founded in 2014 by Cameron and Tyler Winklevoss.

32. Gemini is regulated by the New York State Department of Financial Services.

33. Gemini says that it currently operates in the United States, Canada, the United Kingdom, South Korea, Hong Kong, and Singapore.

34. In May 2021, Gemini announced that it had more than $30 billion in crypto assets under management.

Gemini Falsely Claims to Have a "Security-First Mentality"

35. Gemini assures the public that it is laser-focused on security and protecting the crypto assets with which it is entrusted. The company's website states that:

> [E]very employee at Gemini continues our founders' focus on security and compliance, in order to build trust. Gemini has a built a leading security program focused on developing innovative security solutions to help protect and secure our customers and their assets. We have also invested considerable resources to remain

> transparent about our security posture, through third-party security assessments, including our SOC2 Type 2, ISO 27001, and annual penetration testing.

See www.gemini.com/security.

36. Gemini states that "protecting your crypto is a cornerstone of our mission to build the future of money. We have operated from day one with a security-first mentality and have focused on providing our customers with layered security features to help them protect their Gemini accounts. Simply put, trust is our product." *See* https://www.gemini.com/blog/securing-your-gemini-account-with-webauthn.

37. According to Gemini's website, it purports to "take a number of measures to safeguard your account, like requiring multi-factor authentication and verification of new devices." *See* https://www.gemini.com/trust-and-safety.

38. Gemini also claims that it employs sophisticated means, like "machine learning and customized rules to evaluate signals that help respond to suspicious activity." *Id*.

39. Gemini's website further states, '"The multi-signature digital signature scheme used ***eliminates single points of failure*** and improves our resilience against the loss or compromise of any individual private key. . . . Access to production systems requires use of hardware security keys, which are not susceptible to phishing attacks. . . . Multiple signatories are required to transfer cryptocurrency out of our Cold Storage System and perform other sensitive functions." *See* https://www.gemini.com/security (Emphasis added).

40. Gemini also assures customers that their crypto assets are insured. For example, Gemini's website states that it "maintains coverage for the crypto that we hold on your behalf in our online hot wallet." *See* https://support.gemini.com/hc/en-us/articles/205823016-Are-my-funds-insured-#:~:text=Gemini%20maintains%20insurance%20coverage%20for,User%20Agreement%20for%

20more%20information.&text=Funds%20in%20Gemini%20Earn%20are%20not%20insured%20by%20Gemini.

IRA Relied on Gemini's Misrepresentations

41. In 2019, IRA had the idea to allow individuals to invest in crypto assets directly through a self-directed IRA. At that time, few, if any, self-directed retirement account providers offered this; instead, an individual wishing to invest in crypto assets through a self-directed retirement account needed to create an LLC owned by the retirement account to do so.

42. As part of investigating this possibility, IRA researched and reached out to various crypto exchanges, including Gemini, Coinbase, and Kraken.

43. IRA's business model does not involve taking custody of any assets. In fact, IRA is not licensed to do so. Instead, IRA handles the administrative tasks associated with making sure self-directed retirement accounts are compliant with the various IRS regulations and relies on its custodial partners, such as a regulated exchange, to handle custody of customer assets.

44. In the context of crypto assets, custody means having possession of the private keys for the digital wallets holding the crypto assets. A private key is a long string of digits that is used to sign and authorize transfer of the crypto assets on the relevant blockchain (*e.g.*, Bitcoin, Ethereum).

45. Security over these private keys is particularly important, because whoever has possession of a private key can irrevocably transfer whatever crypto assets are stored in that wallet.

46. IRA thus focused its research on crypto exchanges' ability to secure the crypto assets, which are notoriously subject to theft and fraud attempts.

47. In May 2019, IRA met with Gemini in Gemini's New York office.

48. At that meeting, IRA explained its plan to allow its customers to purchase crypto assets through their self-directed retirement accounts.

49. At all times, Gemini was aware that IRA's customer accounts would be individual retirement accounts.

50. IRA made clear during this meeting that it needed an exchange to be responsible for the custody and security of the crypto assets. IRA would do what it does best—handle the administrative requirements of retirement accounts—while the exchange would bear responsibility for the custody and security of the crypto assets and allow clients to purchase and sell those assets.

51. IRA also made clear that it was not interested in earning commissions on its customers' crypto trades. IRA would simply earn its flat management fees. This meant that Gemini would earn 100% of the commissions for all crypto trades made by the customers.

52. Gemini was very interested in serving as the exchange on which the customers would store and trade crypto assets.

53. Both before and after this meeting, IRA researched Gemini's security practices. IRA relied on the following Gemini statements, all of which appeared on Gemini's website at the relevant time period in 2019:[1]

[1] These snapshots were taken from the Wayback Machine Internet Archive as of mid-2019.

The above linked to a statement from Tyler Winklevoss that included the following:

3. Value Security Over Profit.

To never cut corners. To set the standard and follow best practices in order to provide a platform that is free of hacking and fraud.

Financial crime affects both fiat and cryptocurrencies alike, but the crypto revolution will not succeed if our industry is plagued by nefarious activity. High-profile hacks that result in catastrophic losses must become a thing of the past, and we must shake the image of an industry characterized by poor security standards, internal controls, and policies and procedures.

In an effort to do so, we built our team with a ***security-first*** mentality from day one—a team that has built a state-of-the-art hot wallet and cold storage system and is deeply committed to employing cybersecurity best practices to protect your funds and the integrity of our platform. Recently, we added a further layer of protection by securing insurance coverage for the cryptocurrency that we hold on your behalf in our online hot wallet. We are, and will continue to be, committed to making Gemini a safe and secure platform to store your cryptocurrency.

We are a fiduciary and subject to the capital reserve requirements, cybersecurity requirements, and banking compliance standards set forth by the New York State Department of Financial Services (NYSDFS) and the New York Banking Law.

Importantly, Gemini represented that all institutional funds would be "custodied and secured offline in Gemini's proprietary Cold Storage System":

Gemini offers **Custody Accounts** as a solution to store your digital assets in a regulated, secure, and compliant manner. Custody Accounts are ideal for institutional customers like hedge funds, mutual funds, and exchange-traded funds, who may be ***required by law*** to store their digital assets with a licensed custodian like Gemini. A Custody Account constitutes a bailment relationship between you and Gemini (i.e., you retain title).

In a Custody Account, customer digital assets are segregated, using unique digital asset addresses, which are independently verifiable and auditable on their respective blockchains. All segregated digital assets are custodied and secured offline in Gemini's proprietary Cold Storage System. For more information on our custody services, please refer to our Custody Agreement.

Trust is Our Product™

Protecting your cryptocurrency and your personal information is what we do — it's how we earn your trust. Security is the cornerstone of our culture and we have operated with a security-first mentality from day one. Simply put, **trust is our product**.

OUR CRYPTOCURRENCY SECURITY

The majority of your cryptocurrency is held in our offline, air-gapped Cold Storage system. Only a small portion of your cryptocurrency is held in our fully-insured, online Hot Wallet.

OUR COLD STORAGE SYSTEM

- We use hardware security modules (HSMs) that have achieved a FIPS 140-2 Level 3 rating or higher.
- All private keys are generated onboard our HSMs and stored and managed there for their lifetime.
- We use a multisignature digital signature scheme (multisig) to eliminate single points of failure and improve our resilience against the loss or compromise of any individual private key.
- All HSMs are geographically distributed and stored in monitored, access-controlled facilities.
- All HSMs require the coordinated action of multiple employees to operate.

OUR HOT WALLET

- Our Hot Wallet is hosted on Amazon Web Services (AWS). AWS has a proven track record for physical security and internal controls. More information can be found here.
- We follow the *principle of least-privilege* by applying tiered, role-based access-controls to our production environment. Administrative access requires multi-factor authentication.
- All Hot Wallet private keys are managed in the AWS CloudHSM service, which provides dedicated HSMs in the AWS cloud that have achieved a FIPS 140-2 Level 2 rating.

YOUR ACCOUNT SECURITY FEATURES

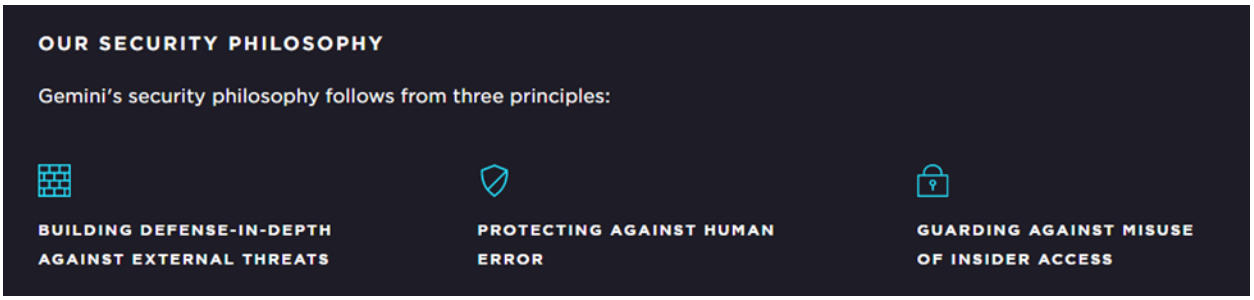
- **Two-Factor Authentication** (2FA) via Authy OneTouch and **Strong Passwords** are required for logging in to your account and making withdrawals.
- **Hardware Security Keys** and **WebAuthn** support allow you to use hardware security keys to secure your account.
- **Address Whitelisting** allows you to block all cryptocurrency withdrawal activity for your account, or restrict cryptocurrency withdrawals to cryptocurrency addresses you whitelist.
- **Rate-limiting** is applied to certain account operations, such as your login attempts, in order to thwart brute force attacks.
- **Encryption** is used to secure your passwords, personal information, and other sensitive information both in transit and at rest.

OUR INFRASTRUCTURE SECURITY

- All of our website data is transmitted over encrypted Transport Layer Security (TLS) connections (i.e., HTTPS).
- We leverage the content-security policy (CSP) and HTTP Strict Transport Security (HSTS) features found in modern browsers.
- We partner with enterprise vendors to mitigate against distributed denial-of-service (DDoS) attacks.
- Internal-only sections of our website have separate access controls and are not exposed to the public Internet.

INTERNAL CONTROLS

- Multiple signatories are required to transfer cryptocurrency out of our Cold Storage System.
- Our CEO (Tyler Winklevoss) and President (Cameron Winklevoss) are unable to individually or jointly transfer cryptocurrency out of our Cold Storage System.
- Our offices do not store or contain anything of value, including private keys. All private keys are stored offsite and geographically distributed in monitored, access-controlled facilities.
- All employees undergo criminal and credit background checks and are subject to ongoing background checks throughout their employment.
- All remote-access requires public-key authentication via credentials stored on hardware tokens — passwords, one-time passwords (OTPs), or other phishable credentials are not permitted.



54. Based on Gemini's representations regarding its security practices, including the statements above, IRA selected Gemini to take custody of and secure the crypto assets and allow the customers to trade their crypto. IRA chose Gemini based on its statements and reputation as a security-focused crypto exchange.

The IRA/Gemini Relationship

55. Following its decision, Gemini sent IRA a questionnaire, which IRA completed.

56. Thereafter, Gemini set IRA up as an institutional customer of Gemini in September 2019.

57. IRA serves as an intermediary, connecting clients that seek to hold crypto assets with Gemini, to Gemini.

58. Gemini originally provided IRA with a web-based interface to allow IRA customers to purchase, store, and trade crypto on Gemini.

59. Under the web-based system, when a customer informed IRA that they want to trade crypto through their retirement account, IRA used the Gemini web-based system to enter the client's name and email.

60. At the same time, the customer filled out the appropriate paperwork allowing IRA to send the client's funds to Gemini once Gemini approved the customer.

61. Gemini required the customer to undergo Gemini's new-customer onboarding process.

62. After IRA entered the customer's name and email in the web-based system, Gemini sent an email directly to the customer that includes instructions about what the customer needed to do to comply with Gemini's "Know Your Customer" requirements, such as uploading proper identification.

63. IRA was not copied on this email or the customer's response, or otherwise involved in the onboarding process; all required information and documentation was sent by the customer directly to Gemini.

64. Once Gemini approved the customer, it informed IRA, which then transferred the customer's funds to a Gemini account at Silvergate Bank.

65. Gemini set up and owned the Silvergate Bank account, which was called "Primary 1," and gave IRA access to that account.

66. IRA sent the customer's funds to that account.

67. Thereafter, a sub-account was created for the new customer, and funds were moved to that customer's sub-account. But these funds were still in Gemini bank accounts; the customer did not open their own account with Silvergate Bank.

68. Once a new client's account was opened at Gemini, the client was free to transact in crypto.

69. Clients performed all of their crypto trading on the Gemini platform.

70. The subject crypto assets resided with Gemini, which had custody over the private keys. Clients received crypto account statements from Gemini.

71. IRA quickly ran into operational issues with Gemini.

72. IRA experienced substantial customer demand for crypto accounts and was referring a large number of customers to Gemini.

73. Soon thereafter, the Primary 1 account filled up.

74. At that time, Gemini created a new Gemini Silvergate Bank account, this one called "Primary 2," to which Gemini instructed IRA to send its customers' funds.

75. Again, Primary 2 reached its maximum capacity quickly.

76. As the parties were experiencing issues with Primary 2, Gemini started pressuring IRA to move from the web-based platform to the Gemini API. Essentially, the Gemini API is a software interface that allows customers to trade crypto.

77. According to Gemini, moving to the API would resolve the account-capacity issue, since there was no limit on the number of accounts that could be opened under the API.

78. On March 31, 2021, Gemini stated to IRA in an email that "API will be a far superior experience for both IRA Financial and Gemini."

79. In the spring and summer of 2021, Gemini and IRA had discussions about transferring to the API.

80. While Gemini continued to pressure IRA to use the API, selling it as an improvement for IRA and the clients, at no time did Gemini identify security issues with moving to the API.

81. On September 8, 2021, based on Gemini's representation and recommendations, IRA started using the Gemini API.

82. IRA customers also reached out to IRA and asked that they be able to remove their crypto assets from the Gemini exchange to store them on their own private digital wallets. These customers expressed concern to IRA about the risks of storing assets on a crypto exchange like Gemini. Their concerns turned out to be prescient.

83. IRA informed Gemini that some IRA clients wanted the ability to store their own crypto assets. In response, Gemini pushed back hard, again referring to the company's robust security features.

84. Additionally, in response to IRA's inquiries about having clients remove crypto assets from the Gemini exchange, Gemini represented to IRA that the crypto assets on the Gemini exchange were insured and that IRA should tell its customers about the insurance:

From: Kristen Mirabella [mailto:kristen.mirabella@gemini.com]
Sent: Friday, February 04, 2022 4:54 PM
To: Deborah Petersen <DPetersen@irafinancialtrust.com>
Cc: Roxane Berens <RBerens@irafinancialtrust.com>; Samantha Scholten <SScholten@irafinancialtrust.com>; Tracy Ham <THam@irafinancialtrust.com>
Subject: Re: [External] RE: URGENT _ additional complimentary withdrawal please

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Deb,

Sure thing - User Agreement linked.
You can point to the coverage of our hot wallet. Please reiterate, to clients who ask, that we can not disclose the amount or percentage of assets that are held in our hot wallet vs the cold on the exchange side, and that the 'hot wallet' insurance covers security events on the broader Gemini platform.
I hope this helps.

Have a great weekend!
Kristen

85. In other words, Gemini specifically told IRA to tell its customers that their crypto assets were insured.

86. IRA relied on Gemini's representations regarding all customer assets and "security events on the broader Gemini platform" being insured.

87. Throughout the API transition process, Gemini focused on allowing for rapid and unlimited client onboarding. At no time did Gemini direct IRA's attention to any security issues that could come with this transition.

88. Gemini disregarded security in favor of quick customer onboarding, which would allow Gemini to earn more commissions. Upon information and belief, Gemini earned many millions in commissions from IRA customers.

89. From IRA's perspective, based on Gemini's communications to IRA, nothing was changing except for the process of onboarding clients.

90. Unfortunately, that turned out to be false.

91. In reality, Gemini designed its API with a fatal flaw that created a single point of failure that could, and did, render all the other so-called security features moot.

92. The flaw was Gemini's master key, which is discussed further below.

The Criminal Theft

93. On February 8, 2022, at approximately 5pm, a police SWAT team responded to IRA's office in South Dakota based on a 911 call of an alleged kidnapping at the office. But there was no kidnapping. The police later informed IRA that they believe the call was a ruse to distract IRA employees.

94. On the evening of February 8, 2022, IRA was notified of suspicious activity on one of its customer's accounts held on Gemini's trading platform.

95. IRA immediately logged into the Gemini system. This takes several minutes.

96. IRA quickly discovered that crypto assets in the customer's account were being transferred to the Gemini account of another IRA customer, John Doe.[2]

97. This shocked IRA, which was not aware that crypto assets could be transferred between customer sub-accounts. Since these were individual retirement accounts, there was no

[2] Name changed to protect client confidentiality.

reason for transfers between those accounts. In fact, such transfers may violate federal law. Gemini never informed IRA that it was possible to transfer assets between customer accounts.

98. Previously, IRA had requested that Gemini provide a phone number to reach Gemini if there was a need for an urgent response. Gemini refused to provide a phone number, and thus IRA could only contact Gemini via email.

99. IRA immediately emailed Gemini requesting that ***all*** customer accounts be frozen. Four minutes later, having not received any response from Gemini, IRA sent a second email asking that all customer accounts be frozen. Eight minutes after IRA's original email, Gemini responded stating that John Doe's account had been frozen. But the remaining accounts remained unfrozen. IRA frantically emailed Gemini requesting a phone call and demanding, again, that all accounts be frozen.

100. Finally, ***after IRA had sent six urgent emails and nearly two hours after IRA's first email***, Gemini sent an update that all accounts had finally been frozen.

101. By this point, approximately $37 million of Bitcoin and Ether assets had been syphoned out of various customer accounts at Gemini and transferred into John Doe's account. The criminals then transferred all the assets out of John Doe's account. Of the total amount, millions of dollars of the assets were stolen *after* IRA had notified Gemini of the problem and requested that Gemini freeze all IRA customer accounts.

Gemini's Security Failures Caused the Damages

102. Following the criminal theft, IRA learned that Gemini's representations about its security protections were false. In fact, Gemini had created a security regime with a single point of failure within its API that allowed the hackers to bypass all of Gemini's so-called protections.

103. Gemini never informed IRA about this single point of failure. Had Gemini done so, IRA would have insisted that it be eliminated, or else IRA would not have agreed to use the API.

104. As discussed above, Gemini represented to IRA and to IRA's customers that it had certain security measures in place. This included, for example:

a. Multifactor authentication ("***MFA***") for account access;

b. MFA for withdrawals;

c. Email confirmation for withdrawals;

d. Withdrawal approval/cancellation options within confirmation emails;

e. Blocks on withdrawals for a certain amount of time after changes made to an account;

f. "Whitelisting" wallet addresses that are permitted to be used for withdrawals;

g. Fraud detection algorithms to detect unusual transaction patterns; and

h. Multi-signature storage of crypto assets to eliminate a single point of failure.

105. Additionally, Gemini represented that most crypto assets were kept in cold storage – *i.e.,* a digital wallet that is not connected to the internet and thus is less susceptible to theft.

106. Following the attack, IRA learned that all of the above representations were false.

107. Gemini set up IRA's account such that IRA was the "master" account and all of Gemini's IRA customers were sub-accounts under the IRA account.

108. Gemini provided IRA with a "master key." Critically, Gemini never informed IRA about the power of this master key.

109. IRA has since learned that whoever possesses the master key can bypass all of the above protections, such as multifactor authentication.

110. Here, unbeknownst to IRA, the hackers were able to gain control of IRA's master key by committing crimes.

111. Once the hackers had the master key, they were able to effectuate thousands of transactions within a very short period, transferring tens of millions of dollars' worth of Bitcoin and Ether into John Doe's account, and then withdrawing all such assets.

112. Again, IRA had no idea about the power attendant to the master key. Had it known, IRA would have insisted that Gemini eliminate this single point of failure.

113. Indeed, not only did Gemini not inform IRA of the master key's power, but Gemini itself treated IRA's master key with slipshod security. For example, when trying to address customer onboarding issues, Gemini personnel exchanged unsecured, unencrypted emails with IRA ***containing IRA's master key***! Rather than clearly and unambiguously informing IRA about the risks associated with the master key and the need to keep that key absolutely secure, Gemini freely transmitted IRA's master key via an unsecured platform. This was contrary to Gemini's representation above that it uses encryption for sensitive information in transit and at rest.

114. Additionally, Gemini knew that these accounts were retirement accounts. There was no reason for assets to be transferred from one retirement account to another, let alone hundreds of accounts transferring tens of millions of dollars' worth of assets in a systematic manner in a short period of time. These were very obviously fraudulent transactions that Gemini

should have noticed and frozen immediately, at a minimum through its claimed use of fraud detection algorithms to detect unusual transaction patterns. But instead, Gemini allowed all these transactions to occur, leading to the theft of tens of millions of dollars' worth of crypto assets.

115. Upon information and belief, and contrary to its representations above, Gemini is taking the position that the stolen crypto assets are not covered by Gemini's insurance.

Gemini Disingenuously Blames IRA For Client Losses

116. Despite Gemini's security failures being the primary cause of the customer's losses, Gemini published false and defamatory statements placing 100% of the blame on IRA.

117. On April 12, 2022, Gemini sent an email to the affected customers stating:

> Hi there,
>
> Thank you for contacting us about your IRA Financial Group ("IRA Financial") account. Please understand that your account, for which the Gemini platform provides certain services, is managed by IRA Financial. On February 8, 2022, IRA Financial's systems were compromised. Notably, only IRA Financial customers were impacted by the incident that IRA Financial subsequently disclosed. No other Gemini platform users suffered any losses in connection with the incident. We understand your concerns and frustrations with the situation. We would like to take this opportunity to give you more information about what we know from our own investigation into the incident.
>
> Gemini provides institutional customers with industry leading security controls. These controls include, but are not limited to, mandatory two-factor authentication with support for hardware keys, Role Based Access Controls (RBAC) for users and Application Programming Interface (API) keys, and approved wallet addresses.
>
> IRA Financial Group was responsible for generating its own application programming interface (API) keys that were required to access the Gemini interface, and IRA Financial assigned scopes and privileges to those API keys that IRA Financial believed appropriate to operate its business. Our understanding is that, as a result of the incident on February 8, 2022, IRA Financial lost control of the master API keys it had generated.
>
> As an additional security measure, Gemini requires that two administrators from IRA Financial approve new addresses before any withdrawals can occur. On February 8, 2022, two legitimate IRA Financial administrators approved the creation of new external wallet addresses that allowed withdrawals of your assets

> to be processed. As presented to Gemini, these actions satisfied all of Gemini's transaction approval requirements and appeared to be authorized transactions made from IRA Financial's known and approved devices.
>
> Ultimately, IRA Financial was offered various security features that they were able to implement based on their needs. Unfortunately, based on our investigation, it seems that on February 8, 2022, IRA Financial's systems were severely compromised.
>
> Like you, Gemini is deeply concerned by the incident at IRA Financial. We encourage you to reach out to IRA Financial for more information concerning any unauthorized use of your IRA Financial account, as well as what compensation may be available to you for any losses.
>
> Kindest regards,
> Gemini

118. This email falsely blames IRA for the clients' losses and, despite Gemini's duty to disclose, does not say a word about Gemini's security flaws and their primary role as the cause of the customers' losses.

119. Upon information and belief, at the time of sending the above email, Gemini was aware of its security flaws and their role in the customers losses. Thus, upon information and belief, Gemini knowingly and maliciously sent this misleading email in a desperate attempt to distract from its own wrongdoing that, if revealed publicly, could ruin Gemini's reputation as the exchange that "set[s] the standard for crypto cybersecurity."

120. This email damaged IRA's relationships with its customers and caused reputational damage to IRA.

121. As a proximate result of Gemini's conduct detailed in this Complaint, IRA has suffered tens of millions of dollars in damage, including, among others: (a) loss of enterprise value; (b) lost profits; (c) reputational/goodwill damage; (d) time and money spent with experts hired to address the consequences of the breach; (e) time and money spent to defend against

client claims; (f) time and money spent responding to inquiries by regulators; and (g) loss of and damage to customer relationships.

COUNT I – FRAUD

122. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

123. This is an action for fraud against Gemini.

124. Gemini made false representations of material fact that caused IRA to select and continue using Gemini as the crypto exchange to handle trading, custody, and security of the customers' crypto assets.

125. As described above, Gemini made material, false statements about its security practices, including:

a. "Recently, we added a further layer of protection by securing insurance coverage for the cryptocurrency that we hold on your behalf in our online hot wallet."

b. "All segregated digital assets are custodied and secured offline in Gemini's proprietary Cold Storage System."

c. Gemini and IRA's mutual customers' Gemini accounts were protected by multifactor authentication; email confirmation for withdrawals; withdrawal approval/cancellation options within confirmation emails; blocks on withdrawals for a certain amount of time after changes made to an account; "whitelisting" wallet addresses that are permitted to be used for withdrawals; fraud detection algorithms to detect unusual transaction

patterns; and multiple-signature storage of crypto assets to eliminate a single point of failure.

d. "Hot Wallet: We follow the principle of least-privilege by applying tiered, role-based access to our production environment. Administrative Access requires multi-factor authentication."

e. "Encryption is used to secure your passwords, personal information, and other sensitive information both in transit and at rest."

f. All customer assets and security events on the broader Gemini platform are insured.

g. Gemini "maintains insurance coverage for the crypto that we hold on your behalf in our online hot wallet."

126. In fact, Gemini set up its API in a manner that allowed the bypassing of the so-called protections. Moreover, the API allowed for transfers between sub-accounts—a glaring vulnerability—and failed to warn IRA about it. Despite its duty to disclose, Gemini failed to inform IRA of the security flaws in its API.

127. When customers expressed concerns over the storage of assets in Gemini accounts, Gemini doubled-down on its misrepresentations regarding the safety of the customers' Gemini accounts by instructing IRA to tell customers that their assets were insured by Gemini.

128. Gemini knowingly made the false representations on its website and elsewhere in the public domain, and failed to disclose the security flaws, with the intent to induce IRA and others to rely upon the false representations and omissions.

129. IRA reasonably and justifiably relied upon the false representations and omissions to its detriment.

130. As a proximate result, IRA has been damaged.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, including punitive damages, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT II – NEGLIGENCE

131. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

132. Gemini owed IRA a duty to use reasonable care to develop, implement, and update its security protections to address known risks. It was reasonably foreseeable that crypto assets would be the target of cyber-attacks.

133. Gemini breached its duty to use reasonable care by failing to provide to IRA an API that was reasonably safe for IRA clients, who are self-directed retirement account holders and required an additional layer of security.

134. The API was fundamentally flawed because it had a single point of failure and lacked reasonable restrictions on the ability to transfer funds between sub-accounts or on the ability to withdraw unlimited amounts daily.

135. Nor did Gemini's platform provide adequate notification of the withdrawals.

136. Gemini failed to employ competent fraud detection algorithms to detect unusual transaction patterns.

137. Further, when the withdrawals were finally detected, Gemini's response times were unreasonable, including because Gemini negligently refused to provide a phone number to IRA—an institutional provider with many clients on whose behalf Gemini custodied crypto assists—to call in such situations. The delay magnified the losses.

138. As a proximate result of Gemini's breach of its duty to IRA, IRA has been damaged.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT III – GROSS NEGLIGENCE

139. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

140. Under the circumstances, Gemini was aware of circumstances constituting an imminent or clear-and-present danger amounting to more than normal or usual peril; attempts to steal cryptocurrency are commonplace. Gemini's many statements about its security protections, though false, evidence its awareness of the clear-and-present danger.

141. Gemini acted, and failed to act, in a manner that evinces a conscious disregard for the consequences of its actions and the damages that would be suffered by IRA.

142. As a proximate result. IRA has been damaged.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, including punitive damages, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT III – VIOLATION OF NEW YORK GBL § 349

143. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

144. Gemini engaged in "consumer-oriented" conduct, namely, the solicitation of customer accounts for the purpose of conducting crypto transactions.

145. In furtherance of that conduct, Gemini engaged in unlawful deceptive acts and practices in violation of New York General Business Law § 349.

146. Gemini engaged in unfair, deceptive, fraudulent and/or unconscionable acts or practices in the conduct of trade or commerce by making false or misleading statements regarding its security practices and insurance to customers, including institutional customers like IRA. These false and misleading statements include:

a. Gemini "value[s] security over profit"

b. "Recently, we added a further layer of protection by securing insurance coverage for the cryptocurrency that we hold on your behalf in our online hot wallet."

c. "All segregated digital assets are custodied and secured offline in Gemini's proprietary Cold Storage System."

d. Gemini and IRA's mutual customers' Gemini accounts were protected by multifactor authentication; email confirmation for withdrawals; withdrawal approval/cancellation options within confirmation emails; blocks on withdrawals for a certain amount of time after changes made to an account; "whitelisting" wallet addresses that are permitted to be used for withdrawals; fraud detection algorithms to detect unusual transaction patterns; and multiple-signature storage of crypto assets to eliminate a single point of failure.

e. "Hot Wallet: We follow the principle of least-privilege by applying tiered, role-based access to our production environment. Administrative Access requires multi-factor authentication."

f. "Encryption is used to secure your passwords, personal information, and other sensitive information both in transit and at rest."

g. All customer assets and security events on the broader Gemini platform are insured.

h. Gemini "maintains insurance coverage for the crypto that we hold on your behalf in our online hot wallet."

147. Gemini made its untrue and/or misleading statements and representations willfully, wantonly, and with reckless disregard for the truth.

148. Gemini's misrepresentations and omissions were material to IRA, which relied upon these misrepresentations and omissions in choosing to do business with Gemini.

149. As a direct and proximate result of Gemini's misrepresentations and omissions, IRA has been damaged.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, including treble damages, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT IV – CONTRIBUTION

150. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

151. IRA's customers have asserted claims against IRA based on the above.

152. To the extent IRA is found liable for such claims, Gemini, which breached its duties to IRA and to the affected customers and whose conduct proximately caused IRA's and the affected customers' damages, must contribute in an amount equal to its equitable share determined based on its relative culpability.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT V – DEFAMATION

153. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

154. As set forth above, Gemini made false and defamatory statements of fact against IRA.

155. These statements tend to injure another in their trade business, or profession and are thus defamatory *per se*.

156. Gemini communicated the defamatory statements to one or more third parties.

157. Gemini's defamatory statements were not privileged.

158. Gemini's defamatory statements were not made in complete good faith.

159. Gemini acted with malice in making the defamatory statements.

160. Gemini made the defamatory statements for the purpose of, without limitation, deflecting culpability for its own role in the security breach.

161. As a proximate cause of Gemini's defamation, IRA suffered damages, including special harm and special damages.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, including special, presumed, actual, and punitive damages, plus interest, costs and such other and further relief as this Court may deem just and proper.

COUNT VI – TORTIOUS INTERFERENCE

162. IRA repeats and realleges each of the allegations set forth in Paragraphs 1-121 as if fully set forth herein.

163. IRA has a business and contractual relationship with its customers.

164. At all relevant times, Gemini was aware of IRA's business and contractual relationship with its customers.

165. Gemini intentionally and unjustifiably interfered with the business and contractual relationship between IRA and its customers by, among other things, sending the email described in paragraph 117.

166. Gemini interfered using improper means, including fraud, and thus is not protected by the competition or any other privilege.

167. As a proximate result of Gemini's interference, IRA suffered damages.

WHEREFORE, IRA demands judgment against Gemini for damages in an amount to be determined at trial, including punitive damages, plus interest, costs and such other and further relief as this Court may deem just and proper.

DEMAND FOR ATTORNEYS' FEES

IRA demands its reasonable attorneys' fees for all claims that so provide.

DEMAND FOR JURY TRIAL

IRA demands a trial by jury on all counts so triable.

Dated: New York, New York
June 6, 2022

MORGAN, LEWIS & BOCKIUS LLP

By: *s/ Peter C. Neger*
Peter C. Neger (NY Bar No. 1792266)
101 Park Avenue
New York, New York 10178
Tel: +1.212.309.6000
Fax: +1.212.309.6001
Email: peter.neger@morganlewis.com

MELAND BUDWICK, P.A.
Eric Ostroff (Pro Hac Vice Forthcoming)
eostroff@melandbudwick.com
Barry Kamar (Pro Hac Vice Forthcoming)
bkamar@melandbudwick.com
Jennifer Greenberg (Pro Hac Vice Forthcoming)
jgreenberg@melandbudwick.com
Alex Brody (Pro Hac Vice Forthcoming)
abrody@melandbudwick.com
3200 Southeast Financial Center
200 South Biscayne Blvd.
Miami, FL 33131
Tel: +1.305.358.6363
Fax: +1.305.358.1221