IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MANNU SINGH, on behalf of himself and others similarly situated, Plaintiffs, v. ILLUSORY SYSTEMS, INC.; ARCHETYPE CRYPTO II, LLC; CONSENSYS SOFTWARE, INC.; CONNEXT LABS, INC.; COINBASE, INC.; OZONE NETWORKS, INC.; POLYCHAIN ALCHEMY, LLC; CIRCLE INTERNET FINANCIAL, LLC, Defendants.	Case No. _____ CLASS ACTION JURY TRIAL DEMANDED

COMPLAINT

Preliminary Statement

1. The Nomad Enterprise runs a business transmitting crypto assets. It classifies its business as a "bridge" because the business allows users to take assets from one crypto blockchain and send them to another crypto blockchain. On August 2, 2022, a malicious individual hacked the bridge and stole approximately $186 million worth of user assets. Defendant Illusory Systems, Inc., which initially created the bridge ("Nomad Bridge"), had promised users that it employed state-of-the-art cryptography to protect user assets. This was an illusory promise. Nomad never implemented many of its supposedly innovative security features; instead, a Nomad programmer introduced a simple mistake into the bridge code, allowing the assets to be stolen; and Nomad ignored obvious signs that a hack was occurring and failed to shut the bridge down. Approximately $172,000 of Plaintiff Mannu Singh's assets were lost or stolen as part of the $186 million theft.

2. Although Illusory Systems created the bridge and operates the website through which users may access it, the Nomad Bridge is controlled by the holders of five cryptographic keys, which are together held by four entities (together "Nomad Defendants"): Illusory Systems, which holds two keys; and Archetype Crypto II, LLC, Consensys Software, Inc., and Connext Labs, Inc. that each hold one key. The Nomad Defendants formed an association-in-fact enterprise to operate the Nomad Bridge without any separate corporate formality or other protection (the "Nomad Enterprise").

3. The Nomad Bridge has not been registered with the Financial Crimes Enforcement Network or with any state regulator. And the Nomad Defendants systematically induced people, including Singh, to part with their money by making knowingly false statements about the Nomad Bridge's security. The Nomad Defendants, therefore, continuously violate 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money-transmitting business, and 18 U.S.C. § 1343,

which prohibits wire fraud. Both are predicate offenses under the Racketeering Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 *et seq.* ("RICO").

4. Defendants Coinbase, Inc., Ozone Networks, Inc., Polychain Alchemy, LLC, Circle Internet Financial LLC, and Archetype Crypto II, LLC (together "Conspirator Defendants"), conspired with the Nomad Defendants to bring the Nomad Enterprise into existence. Before the Nomad Bridge began operations, the Conspirator Defendants agreed to provide funding, guidance, and advice to Illusory Systems in exchange for an ownership in Illusory Systems, which was created to solely participate in the operation of an illegal money-transmitting business. The Conspirator Defendants entered this agreement for the sole purpose of creating the Nomad Enterprise's illegal business.

The Parties

5. Plaintiff Mannu Singh is a Canadian citizen residing in Montreal. Approximately $170,000 of his assets were lost or stolen by the Nomad Enterprise.

6. Defendant Illusory Systems, Inc., is a Delaware corporation with its principal place of business in Centerville, Utah. Illusory Systems founded and created the Nomad Bridge and holds two of the five keys necessary to govern it.

7. Defendant Archetype Crypto II, LLC, is a Delaware limited liability company headquartered in New York City. It operates a venture capital fund and holds one of the five keys necessary to govern the Nomad Bridge. It also agreed in 2022 to provide funding, advice, and guidance to Illusory Systems in exchange for an ownership share in its illegal money-transmitting business.

8. Defendant Consensys Software, Inc., is a Delaware corporation headquartered in New York City. It operates a crypto software and advisory firm and holds one of the five keys necessary to operate the Nomad Bridge.

9. Defendant Connext Labs, Inc., is a Delaware corporation headquartered in San Francisco. It operates a blockchain software company and holds one of the five keys necessary to operate the Nomad Bridge.

10. Defendant Ozone Networks, Inc., is a Delaware corporation headquartered in New York City. It principally operates an online exchange called OpenSea, on which users can trade non-fungible tokens, which are a form of digital collectible. In 2022, Ozone agreed to provide funding, advice, and guidance to Illusory Systems in exchange for an ownership share in its illegal money-transmitting business.

11. Defendant Coinbase, Inc., is a Delaware corporation headquartered in San Francisco. It principally operates an online exchange for crypto assets, and in 2022, it agreed to provide funding, advice, and guidance to Illusory Systems in exchange for an ownership share in its illegal money-transmitting business.

12. Defendant Polychain Alchemy, LLC, is a Delaware limited liability company headquartered in San Francisco. It principally operates a venture capital fund, and in 2022, it agreed to provide funding, advice, and guidance to Illusory Systems in exchange for an ownership share in its illegal money-transmitting business.

13. Defendant Circle Internet Financial, LLC, is a Delaware limited liability company headquartered in Boston. It principally operates U.S. Dollar Coin, a convertible digital currency, and, in 2022, it agreed to provide funding, advice, and guidance to Illusory Systems in exchange for an ownership share in its illegal money-transmitting business.

Jurisdiction and Venue

14. The Court has subject matter jurisdiction over this Action under 28 U.S.C. § 1331 because it arises under the laws of the United States, and under 28 U.S.C. § 1332(d)(2) because this is a putative class action in which: (a) at least one member of the Plaintiff Class is a foreign

citizen, (b) all Defendants are citizens of a State, and (c) the amount in controversy exceeds $5,000,000. The Court may also exercise supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

15. The Court may exercise general personal jurisdiction over all Defendants because each is incorporated in Delaware.

Background on the Relevant Technology

16. A blockchain is a system for a distributed network of machines to maintain a ledger of transactions publicly and securely. The most famous blockchain is Bitcoin, which exists to facilitate transactions in its eponymous crypto asset. But there are many others, most prominently Ethereum. Users participate in blockchains using wallet addresses, which are digital representations of the sending and receiving ends of transactions on the blockchain.

17. A crypto asset is a form of digital asset traded on a blockchain. Crypto assets are not currently issued by central governments or authorities. The value of some crypto assets fluctuates with respect to the U.S. Dollar and all other currencies. Other crypto assets, such as U.S. Dollar Coin, are so-called "stablecoins" because their value is pegged to a government currency—for U.S. Dollar Coin ("USDC"), the U.S. Dollar. A unit of a crypto asset is called a "token."

18. Some blockchains, such as Ethereum, allow users to conduct transactions using "smart contracts." Smart contracts are pieces of software that automatically execute transactions when certain conditions are triggered. For example, an individual may create a smart contract that sends one crypto asset to a specific wallet address whenever it receives another crypto asset. A real-world example of a smart contract is a vending machine—a user inserts money, and the machine releases an item, even though no two parties ever manifested their assent to the agreement in a person-to-person interaction.

19. Blockchains are secure because each new series of transactions (a "block") is added to all prior series of transactions (hence a "chain") in a way that makes any changes to old transactions immediately visible. No two blockchains will ever have the same series of old transactions, therefore it is technologically impossible to transfer assets from a wallet address on one blockchain to a wallet address on another blockchain directly.

20. As the market for digital assets grew over the past three or four years, so did the number of public blockchains. For example, because the Ethereum blockchain is comparatively slow and expensive, some users began conducting their transactions on other chains that are similar to but faster than Ethereum. Meanwhile, Bitcoin, the most popular and generally most valuable digital asset, cannot be traded on Ethereum, the most popular smart contract-capable blockchain.

21. Cross-chain bridge services arose to solve the problem of blockchain interoperability. Through a bridge, users can effectively send assets from one chain to another. Technologically, a bridge does this in two steps. First, the bridge uses a smart contract on the origin chain to record an outgoing transaction, which effectively freezes or escrows the asset on the first chain. Second, the bridge uses a smart contract on the destination chain to record an incoming transaction, which creates a new asset on the second chain entitling the user to an equivalent amount of the old asset. These new assets are generally called "wrapped" assets.

22. Unlike blockchains themselves, though, bridges need not be (and generally are not) distributed across a wide network of machines that securely and publicly record transactions. Instead, they take possession of users' funds on one chain to transmit them to another. And thus arises a cryptographic problem—like bridges in a war, bridges between blockchains are narrow and highly valuable pathways. For this reason, many bridges have recently been hacked, resulting in billions of dollars of worth of losses.

Defendants Conspire to Form Nomad

23. Pranay Mohan, Barbara Liau, and James Prestwich have worked in various capacities in the crypto industry since 2017. Between 2017 and 2021, they researched various cryptographic mechanisms to conduct cross-blockchain transactions. Through that research, they eventually settled on a cryptographic idea called "optimism," which (roughly speaking) is a cryptographic system that presumes propositions to be valid unless proven otherwise by a verifying party. Optimism, they contended in a 2021 blog post, was a "breakthrough" that they could use to "construct a more trust-minimized bridge that is also easy to deploy across varied ecosystems."

24. In 2021, Mohan, Liau, and Prestwich decided to create a new cross-chain bridge based on the optimism idea and to call it "Nomad." The goal was to create a system by which users and companies could create applications across chains. Their own flagship application was called the Nomad Bridge, and it was designed to be a "token bridge"—that is, a bridge that exists to move crypto assets between blockchains. Mohan, Liau, and Prestwich emphasized in a blog post that the bridge was created in response to users' need to safely move "liquidity" between blockchains, which had previously been done by "apeing"—an evidently insecure process—or through "hastily constructed" bridges.

25. On November 10, 2021, they incorporated Illusory Systems in Delaware.

26. Through the end of 2021 and beginning of 2022, Illusory Systems worked to develop the software underlying the Nomad Bridge.

27. At the same time, Illusory Systems solicited capital to operate the business.

28. On April 12, 2022, Illusory Systems announced that it had raised $22 million in a "seed round" led by Polychain with participation from Archetype, Circle, Coinbase, and 26 other, smaller companies. Later, on July 28, 2022, Illusory Systems announced that it had raised more money in a second round, this time including participation from Ozone.

29. The Conspirator Defendants agreed to provide Illusory Systems funding for the purpose of enabling Illusory Systems to create the Nomad Bridge and in exchange for a share of the profits from operating that bridge.

30. The Conspirator Defendants further agreed to help Illusory Systems operate the bridge. For example, Circle explains on the website for its venture project that "Founders [of companies that Circle invests in] get much more than capital. We also deliver . . . expertise to help you explore product synergies and collaboration with Circle . . . ."

31. Ozone explains that companies in which it invests will get "direct access to [its] leadership."

32. Coinbase explains on the website for its venture project that "[w]e strive to be strategic partners for founders and take a collaborative approach to investing. We support founders through operational experience, distribution, strategic partnerships, and more."

33. The Conspirator Defendants knew that Illusory Systems' only business was the Nomad Bridge.

34. The Nomad Defendants' executives were aware that they were required to comply with federal laws related to their business. An April 2022 statement from Illusory Systems' CEO explained that they "have to follow" the U.S. Department of Treasury's Office of Foreign Assets Control rules. Similar statements were made by Illusory Systems' COO in January 2022. And at least Circle and Coinbase also knew that running a business transmitting crypto assets is illegal without registration, in light of the fact that both Circle and Coinbase hold money-transmitter licenses for other parts of their business in almost every state, and both are registered with the U.S. Treasury Financial Crimes Enforcement Network ("FINCEN").

Nomad's Criminal Enterprise

35. The Nomad Enterprise continuously violates 18 U.S.C. § 1960, which prohibits the operation of an unlicensed money-transmitting business, and 18 U.S.C. § 1343, which prohibits wire fraud, by operating the Nomad Bridge and by inducing people to use it through knowingly false promises of security.

36. Through the Nomad Bridge, a user can move assets between the Ethereum, Avalanche, Evmos, Milkomeda, and Moonbeam blockchains.

37. To use the Nomad Bridge, users simply navigate to nomad.xyz (a website operated by Illusory Systems), link a crypto wallet to the bridge, select the assets they want to send and where they want to send them, and then click send. Nomad will transmit many different crypto assets including many stablecoins, Bitcoin, and Ether (the native asset of the Ethereum blockchain).

38. At no point during this process are users required to provide their names, residences, or identification. And at no point do users have to identify themselves at all. There is no limitation on the amounts users can send or to whom they can send them. Illusory Systems' website does not limit participation based on location, so users from Iran, North Korea, and other sanctioned nations can access the Nomad Bridge so long as they are able to transfer information out of their home countries.

39. Although most users access the Nomad Bridge through Illusory Systems' website (called a "front-end interface" in the crypto community), it is in fact governed behind the scenes by the Nomad Defendants and works as follows.

The Nomad Smart Contracts and Their Stated Functions

40. To begin the process of transferring money from, for example, Chain A to Chain B, a user begins by sending assets to a smart contract called Home, which functions as the outbox for transactions on Chain A.

41. Using a cryptographic process known as Merkle tree functions (by which the validity of a message, a "branch," is determined by its relationship to prior messages, called "roots"), the Home contract, according to a technical whitepaper on Illusory Systems' website, "permissions an Updater . . . that must attest to the state of the message tree."

42. An "Updater" is a piece of software run by the Nomad Enterprise—it is not a smart contract and is not part of any blockchain. Illusory Systems describes the Updater as an "off-chain agent."

43. To begin a transaction, Illusory Systems' website explains, "[t]he updater places a bond on the Home [contract] and is required to periodically sign updates. Each update contains the root from the previous update . . . and a new root [for future transactions]."

44. The Updater periodically sends the assets it has collected from the Home contract on Chain A to a contract on Chain B called "Replica," which functions as the inbox for Chain B transactions.

45. "Before accepting an update," Illusory Systems' whitepaper explains, "a Replica places it into a queue of pending updates. Each update must wait for some time parameter (the optimistic dispute window) before being accepted."

46. The optimistic dispute window is, according to Illusory Systems, the core innovation of Nomad. During the dispute window, other off-chain software agents, called "Watchers," have the capacity to void any transaction if it does not appear legitimate. The dispute

window is "optimistic" because, unlike other cryptographic techniques, Nomad's system assumes a transaction is valid unless proven otherwise by a Watcher.

47. Thus, according to Illusory Systems, the system as a whole is secure. If *any* Watcher objects or if the Updater "attempts to commit fraud," the transaction is cancelled and that Updater is "slashed," or punished financially. This makes sense as a cryptographic matter if and only if the Updaters, or at least one Watcher, is assured to be trustworthy or is subject to a set of incentives that makes dishonest or incompetent conduct very unlikely. Nomad advertises itself as committed to minimal-trust cryptography—that is, cryptography that does not ever rely on trusting another entity to behave honestly—so the Watchers and Updater will function only if there is some incentive built into the system for them to be honest.

Nomad "Governance"

48. The Home and Replica contracts—the "on chain" portions of the Nomad system—are controlled by a smart contract called "Nomad Governance."

49. Nomad Governance is considered a "safe" created by a company called "Gnosis." Gnosis safes are contracts that allow a group of wallet addresses to hold assets together and to specify the conditions under which they will be moved. Nomad Governance is a three-of-five Gnosis safe, meaning there are five wallets with keys to the safe, and three of those keys are required to take any action.

50. The five wallets with the keys are listed on Illusory Systems' website as belonging to Layne Haber, Praneeth Srikanti, Katherine Wu, Pranay Mohan, and Anna Carrol.

51. Carroll and Mohan run Illusory Systems.

52. Wu is a partner at Archetype.

53. Srikanti is an employee of Consensys.

54. And Haber is the founder of Connext.

55. According to Illusory Systems, Nomad Governance also controls the Updaters. "Updaters are selected and enrolled on the Home contract by the UpdaterManager contract," says Illusory Systems' whitepaper. "The UpdaterManager can be changed by calling _setUpdaterManager. This function can only be called by the owner role, which belongs to Nomad governance. At a given time, there is only one Updater enrolled per Home contract."

56. Nomad Governance is empowered at any time to shut the system down.

The Watchers Do Nothing and There is No Slashing Mechanism

57. As explained above, the Updater is the off-chain agent responsible for attesting to the accuracy of transactions, and Watchers are meant to monitor the Updater. The Nomad system supposedly works because there is a window (about half an hour) within which any Watcher can void a transaction. This window should deter the Updater from dishonesty and incompetence because the Updater does not want its "bonded" funds slashed. These are the funds it ostensibly puts at risk whenever it verifies a transaction.

58. Yet, there is no system for selecting Watchers or creating any incentives for them, and none have ever publicly appeared.

59. The Updater "bonding" process never puts any bonded funds at risk, ever.

60. And there is no mechanism to slash Updaters, which are chosen by Nomad Governance and do not have any independence from the Nomad Defendants. "The slashupdater function in the UpdateManager," Illusory Systems states in its technical "white paper" posted on its website before the Nomad Bridge opened, "will be implemented when updater bonding and rotation are also implemented in the future." That future never came.

61. In other words, the core function of Nomad—the only thing separating it from simply trusting five companies with customers' money—does absolutely nothing. The "Optimistic" system that Mohan, Liau, and Carroll created and repeatedly touted fails to protect

user funds that Nomad Governance does not simply do for itself, and indeed the system does nothing to protect the funds *from* the Nomad Enterprise itself.

The Nomad Defendants Formed a RICO Enterprise Operating Through a Pattern of Illegal Money Transmission and Wire Fraud

62. Acting together, the five holders of the keys to the Nomad Governance gnosis safe operate the Nomad Enterprise. With these keys, the Nomad Enterprise can do anything its operators wish with the assets users send to the Home contracts—the key holders, in other words, receive and possess those assets. And because there is no limitation on what the Updater can do and no one other than the people holding the keys to Nomad Governance can alter or control the Updater, there is no possible limitation—and none in fact—on the power that the entities operating the Nomad Enterprise have with the assets it controls.

63. The Nomad Enterprise is operated by the Nomad Defendants (who are those holding the keys to Nomad Governance). They receive crypto assets, which are funds, for the purpose of transferring those funds from a customer's wallet on one blockchain to the customer's wallet or another person's wallet on another blockchain. Illusory Systems advertises these services to the public using its website, where any person can log on and send funds to any other person without identification or verification.

64. The Nomad Enterprise's transactions are themselves interstate or foreign commerce, and therefore affect interstate or foreign commerce.

65. Neither the Nomad Enterprise nor any of the Nomad Defendants hold a money-transmitting license for this purpose in any state. And none of the Nomad Defendants has registered with FINCEN for this purpose.

66. The Nomad Defendants therefore operate an illegal money-transmitting business in violation of 18 U.S.C. § 1960.

67. The Nomad Defendants induce their users to participate with abundant false promises of security made using the internet. Each of those promises is an act of wire fraud under 18 U.S.C. § 1343.

68. Illusory Systems' website has, since the Nomad Bridge's launch, continuously read: "In order to ensure that message-passing [between chains] is secure, Nomad uses an optimistic verification mechanism. . . . This makes Nomad more secure . . . compared to validator/proof-of-stake based interoperability protocols."

69. The Nomad Defendants made many representations about the system's security before and after the Nomad Bridge launched. In January 2022, for example, Illusory Systems' COO said to users: "Nomad isn't designed to be the fastest bridge, but it is designed to have a high level of security, so even if funds take a while, you can at least know they will arrive."

70. On March 29, 2022, Prestwich wrote a message on Twitter reading (emphasis in original): "because watchers can only *revoke* access, and can't *permit* access, compromising the update[r] and 100% of watchers still won't allow theft. an attacker with ALL system keys can't steal funds." As Prestwich surely knew, however, an attacker with "ALL system keys" could change the smart contracts holding the assets and accordingly, could steal *all* funds.

71. Illusory Systems' website has, since the Nomad Bridge's launch, continuously read: "Nomad minimizes the chance of fraud by guaranteeing that: Fraud is easily observed by anyone[,] and [f]raud is costly[:] Anyone can slash a fraudulent updater. [And] [f]raud will be blocked[:] Permissioned Watchers can block Fraud before it takes effect in order to protect applications."

72. In April 2022, an Illusory Systems senior employee told users that the Nomad Bridge is "the most secure way to bridge your assets anywhere," "it is the most secure way to send

packets from one chain to another," and "our job is to just get your assets from one chain to another in the most secure way possible[.]"

73. And Illusory Systems' CEO repeatedly told users their funds were safe and encouraged them to leave funds in the bridge for longer periods of time, including several times in April and May 2022: "If you have already bridged back to Ethereum, all you need to do is claim your funds. They are safe, and you can wait til fees are lower." "[D]on't worry [username] – your funds are safe, lot of network traffic due to evmos launch[.]" "[T]ake your time, you can always claim when gas fees are lower. . . funds are safe and stored in contracts[.]"[1]

74. In May 2022, Illusory Systems' CEO made repeated statements about the Nomad Bridge's security on a podcast promoting Nomad including:

- "Nomad's whole design model is predicated on being able to offer enough security and basically focus on the user to give them what they need."
- Comparing Nomad's focus on security to the focus on security of transatlantic flights: "When you need to go inter-cluster that's where security matters and so I said this on another podcast but I would consider it like a transatlantic flight, right, what matters is getting there safely and not necessarily quickly. Like if you want to be quick you could be shot out of a cannon but you won't get there as safely as if you take, like, a flight and you don't mind 30 minutes because you have other goals to accomplish. You want to get there in one piece and then do business and then come back. I imagine most economic activity in the future in crypto will be within clusters but there will be inter-

[1] Every transaction in a crypto asset using the Ethereum blockchain requires transactors to pay something called a "gas" fee to compensate the network for processing the transactions. Because gas fees are roughly proportional to the volume of transactions happening on the network, they tend to be lower outside business hours in the United States and Europe.

cluster activity and that's where we need to make sure that those channels are secure because the packets being transferred between them will naturally be of higher value and may not represent more frivolous use cases."

- Implying that the Nomad Bridge was better prepared for "Black Swan" events than other bridges and acknowledging that it was unrealistic to expect bridge users to do their own security due diligence: "Expecting users to go and do diligence on all of these bridges and in fact any infrastructure that they use is kind of untenable right. It just really doesn't scale well if every time you drive your car you have to understand deeply how the engine works. . . . Nasim Talib [has] this chart that's like it plots the happiness of a turkey versus the number of days and then you just see it rises linearly and then one day it drops off and the annotation for that day on the x-axis is it's Thanksgiving, right. And so that's what a lot of these bridge hacks have been like where they're humming along just fine, the TVLs [a measure the total value in the bridge] are enormous, they have nine figures or billions of dollars until there is something that goes wrong as a 'Black Swan' risk and then users have a really bad time. But expecting a user to take into account a black swan risk I think is a losing proposition. . . . But if more of these type of hacks start happening we will need to either focus on security ourselves as an industry and prove that we can mature or we are basically asking regulators to come in and say why does this industry keep experiencing nine-figure losses, right?"

75. On July 22, 2022, Illusory Systems stated on its official Twitter account: "There've been many attacks all across the blockchain space over the years. At Nomad, we've been laser-

focused on security innovation, first and foremost, to defend the safety of every anon." Anon is a term that is used to describe the wallets of users.

76. In a July 28, 2022, announcement on *Business Wire*—days before the loss of customer funds—Mohan said that "Nomad's optimistic security model is the gold standard for trust-minimized cross-chain communication." The announcement further read that "Nomad's protocol is tackling [security problems] head-on, utilizing optimistic verification to provide a high level of security that allows watchers to challenge messages via on-chain fraud proofs, without relying on custodians or validators. Unlike validator-based cross-chain bridges, Nomad only requires a single honest watcher to keep the entire system safe." And it included a quote from Illusory Systems' Chief Technology Officer stating, "Our protocol accelerates the adoption of cross-chain communications to help bridge siloed defi ecosystems together in the most secure and cost-efficient way."

77. When the Nomad Defendants prominently advertised the bridge's security features in *Business Wire*—and in all prior public statements—they knew *none* of those security features had been implemented.

78. According to a security audit conducted between April and June 2022 by a firm called Quantstamp, "[t]he correct operation of the system is completely reliant on external agents performing crucial tasks." "In the future," the auditors wrote, "[the Nomad team] will decentralize [the Updater] role and will introduce the necessary mechanism for selecting and rotating the Updater. Until then, the Updater is being operated by the Nomad team itself . . . ." The audit went on to explain that if the governance keys are compromised, users' tokens could be stolen from the home contract on the origin chain without corresponding wrapped tokens issuing on the destination

chain. The audit said, referring to the vulnerability of the Updater, that "[t]he Nomad team is aware of this issue."

79. The Nomad Bridge was founded by experts in cryptography, and those individuals explicitly advertised, for example, "permissioned . . . Watchers" and "bonded . . . Updaters" subject to potential "slashing" as a key feature of its design that never materialized.

80. The Nomad Defendants operated an illegal money-transmitting business and committed wire fraud continuously from late 2021 at least until August 2, 2022, when the Nomad Bridge temporarily shut down.

81. During the nine or ten months that it was fully operational, the Nomad Bridge moved more than $912 million worth of crypto assets on behalf of more than 21,000 unique wallet addresses.

Nomad Loses or Steals $186 Million Worth of Crypto Assets

82. On June 21, 2022, someone working on behalf of the Nomad Defendants introduced a routine update to the Replica contract.

83. Perhaps negligently or perhaps maliciously, that person introduced a vulnerability in the Merkle tree function used by the Replica contract.

84. That vulnerability allowed anyone who saw it to craft transactions to steal funds from the Nomad Bridge without attestation from the Updater because the root of an unattested message is composed of all zeroes, and a message with a zero root was erroneously considered to be a valid message.

85. On or around August 1, 2022, someone executed a few small fraudulent transactions on Nomad's Replica contracts, stealing a small amount of money.

86. Had the Nomad Defendants been exercising due care to monitor the system, they could have shut it down or fixed the vulnerability and thereby stopped any future theft.

87. Instead, the Nomad Bridge stayed open, and on August 2, 2022, a malicious actor began executing fraudulent transactions using Nomad's Replica contracts. Through the vulnerability introduced by the Nomad Defendants, and because there was no oversight to shut it down when the thefts were occurring, the malicious actor was able to manipulate the Nomad Bridge contracts on Ethereum to issue all the money to the malicious actor through a process called "spoofing."

88. Once others saw the spoofing—because all blockchain transactions are public—they joined in as well. By the end of the day on August 2, the original malicious actor and many copycats had completely drained the assets in the Nomad Enterprise's possession, resulting in a loss of more than $186 million worth of crypto assets.

89. Introducing the zero-root vulnerability, assuming it was not maliciously introduced, was grossly negligent. The coder who introduced the vulnerability, for example, unnecessarily made the vulnerable function in the Replica contract "publicly callable," which meant that anyone could use it to steal assets. And almost immediately after the hack, a Twitter user going by "samczsun" identified exactly the problem and noted that it resembled other earlier hacks, suggesting that the Nomad Defendants should have known better.

90. It is plausible that the malicious actor worked on behalf of the Nomad Enterprise. Nomad Governance had no protocols in place to double check software updates—once chosen by the Nomad Defendants, one person could control a blockchain address called the "Deployer" that in fact executed the update—and the Nomad Defendants set up the whole system without adequate safeguards.

91. The zero-root vulnerability is easy to exploit once observed, and easy to avoid, but comparatively hard to find. Someone who knew it was there—such as the person who put it there—would have had a much easier time exploiting it than someone who did not.

92. And indeed this very hack disproves Prestwich's statement that someone with "ALL of the keys" to Nomad Governance could not steal any of the funds. On the contrary, any three governance keyholders could steal all of the money, simply by changing the smart contracts over which they had full control.

Singh's Transactions and Losses, and the Harm to The Class

93. Mannu Singh is a Canadian crypto investor. Like many others, he uses bridges to maintain his investments in a low-cost, high-efficiency way.

94. Singh used the Nomad Bridge three times in June and July 2022 to transmit Ether from the Ethereum blockchain to the Moonbeam blockchain. Singh used nomad.xyz all three times.[2]

95. Singh relied on the Nomad Defendants' promises of security. Had he known that the Nomad Enterprise was in fact not employing any of the innovative security measures the Nomad Defendants had promised, he never would have sent his assets through Nomad.

96. On August 2, 2022, approximately 105 ETH (units of Ethereum) were stolen from Singh during the hack, which was then worth $172,000.

97. That same day, approximately $186 million worth of crypto assets were stolen from members of the class.

[2] Singh pleads approximate dates and numbers here so that the public will not be able to determine his wallet address by comparing his transactions with those pleaded here.

98. This harm was the direct result of the Nomad Enterprise's pattern of racketeering activity.

99. Had the Nomad Enterprise sought a money-transmitting license to operate the bridge, it would almost certainly have been denied. To get a money-transmitting license in New York, for example, businesses must submit compliant anti-money-laundering and know-your-customer policies, which the Nomad Defendants obviously cannot do, and obtain a bond, which no reasonable surety would issue. And had the Nomad Enterprise somehow obtained a money-transmitting license, it would have fallen under the supervision of the New York Department of Financial Services, which would have required the Nomad Defendants to explain its plan for transmitting funds and ensure the security of that plan.

100. Only by violating 18 U.S.C. § 1960 was the Nomad Enterprise able to run its business, and thereby harm Singh and the members of the class.

101. Further, the Nomad Enterprise was able to operate at all only because it falsely promised users that it employed the "gold standard" of cryptographic security, as Mohan put it, while knowing that its security was worthless.

102. The Nomad Bridge, after all, offers nothing other than the security of its process. Users would never put their funds through the bridge if they knew it was insecure and the market would never accept the value of wrapped assets issued by the Nomad Bridge if it knew that they were not reliably exchangeable for the original crypto assets.

103. The Nomad Enterprise's violations of 18 U.S.C. § 1343 directly caused harm to Singh and the class members.

Illusory Systems Returns Some User Funds

104. Since the Nomad Defendants lost or stole approximately $186 million worth of crypto assets, they have supposedly managed to recover some and have begun the process of returning them to users.

105. Immediately after the funds were taken on August 2, 2022, Illusory Systems employees began communicating with wallet addresses that held stolen funds.

106. Illusory Systems told the holders of these wallets that they could keep 10% of the money they had—which they presumably stole—and that Illusory Systems would forego "legal action" against them if they returned the other 90%.

107. People who agree to such terms are called, in the crypto community, "white-hats," alluding to cowboy stories of yore, where riders in white hats were the good guys. White hats sometimes find exploitable code in computer programs to help others maintain safe systems.

108. Through this process, the Nomad Enterprise has been able to recover approximately $36 million worth of stolen assets.

109. Since August 2022, the Nomad Enterprise told users that it is in the process of getting that $36 million worth of stolen assets back to users pro rata to their losses. To do this, the Nomad Enterprise had to fix the bug in the Replica contract and set up a system for users to claim their pro-rata share of the $36 million and any further amounts recovered.

110. Two weeks after the hack, Illusory Systems announced that it would follow a three-phase plan for recovery, which included: "(1) funds recovery, (2) bridge upgrades, and (3) bridge restart/recovered funds distribution." Illusory Systems estimated the bridge would reopen and allow users to begin collecting stolen funds by September. However, this process stalled for several months, during which time Illusory Systems offered vague and varying explanations, such as

pointing to "a timeline set by the auditors," and stating that "Legal needs to ensure that any plans are legally feasible in a regulatory landscape that shifts daily / weekly."

111. It was not until December 20, 2022, that the Nomad Bridge finally allowed some users to attempt to recover a small portion of their stolen funds via a process established by Illusory Systems. But Illusory Systems continued to rebuff inquiries from users about its plans for future recovery and a full reopening. On January 15, 2023, Illusory Systems said that "we will have an update on next steps, it just won't be for several weeks."

112. Remarkably, now that it needs to return the money, the Nomad Enterprise refers to U.S. anti-money-laundering rules. Although it was happy to accept funds for transfer without any know-your-customer process when it was running the bridge, it is now demanding that all customers who seek to recover their funds satisfy a self-described "KYC" (know-your-customer) process.

113. Among the Nomad Enterprise's explanations for only now implementing a KYC requirement for users are that "OFAC [Office of Foreign Assets Control] sanctions . . . ha[ve] become substantially more aggressive since the exploit," and later, that "Nomad needs to ensure that no money passes from us to an entity in a sanctioned country. The only way to be completely sure of that is if we KYC the people that are allowed to bridge back."

Class Action Allegations

114. Singh proposes to move to certify the following class: All people whose crypto assets were lost or stolen on or around August 2, 2022, from the Nomad Bridge.

115. The proposed class meets Federal Rule of Civil Procedure 23's requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

Numerosity

116. The class is so large that joinder of all parties would be impracticable.

117. Many thousands of people had their assets stolen on August 2, 2022, from the Nomad Bridge.

Commonality

118. There are questions of law and fact common to members of the class.

119. The common questions of fact include, without limitation, whether the Nomad Enterprise's representations about security were false, and whether and to what extent they failed to provide the security promised.

120. The common questions of law include, without limitation, whether the Nomad Enterprise's conduct was negligent, whether it constituted a pattern of illegal money transmission, and whether it constituted the creation and operation of an enterprise within the meaning of RICO.

Typicality

121. Singh sent assets to the Nomad Bridge for the purpose of transmitting them from one blockchain to another blockchain and those assets were stolen on August 2, 2022.

122. Every other member of the proposed class sent assets to the Nomad Bridge for the purpose of transmitting them from one blockchain to another blockchain and those assets were stolen on or around August 2, 2022.

123. Singh's claim is typical of—indeed identical to—the claims of all other members of the proposed class.

Adequacy

124. Singh's claim, as explained above, is identical to the claims of other class members and he has no known conflicts of interest with any other class member. Additionally, Singh has experience in the market for crypto assets, which will help him guide this litigation effectively.

125. Singh will adequately protect the interests of absent class members.

126. Singh proposes Gerstein Harrow, LLP, Gupta Wessler, PLLC, and Fairmark Partners, LLP, as class counsel. All three firms are experienced in litigating class actions or matters involving similar or the same questions of law.

127. Class counsel will fairly and adequately represent the interests of the class.

Predominance and Superiority

128. The questions of fact and law common to the class predominate in this action over any questions affecting only individual members of the class.

129. A class action is superior to other available methods for fairly and efficiently adjudicating the plaintiff's claims. Joinder of all members is impracticable, and there will be no difficulty in the management of this case as a class action. Every transaction involving Nomad is publicly recorded and immutable.

Claims for Relief

Count One: Violation of the Racketeering Influenced and Corrupt Organizations Act, 18 U.S.C. 1962(c) (Against the Nomad Defendants)

130. Singh incorporates all prior paragraphs by reference here.

131. The Racketeering Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(c), makes it "unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt."

132. The Nomad Enterprise exists for the purpose of operating the Nomad Bridge, which is an illegal money-transmitting business in violation of 18 U.S.C. § 1960. Conduct violating 18 U.S.C. § 1960 constitutes racketeering under 18 U.S.C. § 1961.

133. The Nomad Enterprise further continuously commits wire fraud by knowingly telling users that its service is cryptographically sophisticated and secure when in fact it employs no valuable cryptographic technology at all. Conduct violating 18 U.S.C. § 1343 constitutes racketeering under 18 U.S.C. § 1961.

134. The Nomad Enterprise is an association-in-fact enterprise governed by the Nomad Defendants, each of which participates in the affairs of the enterprise through a pattern of illegal money transmission in violation of 18 U.S.C. § 1960.

135. Each of the Nomad Defendants further participates in wire fraud by knowingly implementing useless cryptographic technology while knowingly telling users that it is secure.

136. The Nomad Defendants' racketeering activity proximately caused Singh's and the class members' financial loss. That loss is readily ascertainable—*i.e.*, Singh lost approximately $172,000 worth of Ether from the Nomad Enterprise's illegal money-transmitting business, and the proposed class lost $186 million, when it was stolen from them in August 2022. There is no risk of double recovery because the damages Singh and the class seek are the assets that the Nomad Enterprise lost or stole, and there are no other victims or identifiable defendants to make the class members whole. And there are no individuals better situated or incentivized to pursue the monetary relief Singh and the class seek here, because theirs were the assets that were lost.

***Count Two*: Conspiracy to Violate the Racketeering and Influenced Corrupt Organizations Act, 18 U.S.C. 1962(d) (Against All Defendants)**

137. Singh incorporates all prior paragraphs here by reference.

138. The Conspirator Defendants agreed with Illusory Systems and each other to give Illusory Systems money, guidance, and advice for the purpose of facilitating its participation in and creation of the Nomad Enterprise.

139. The Conspirator Defendants did this with the purpose of facilitating an enterprise to operate an illegal money-transmitting business—indeed that was the Nomad Bridge's only possible use.

140. Singh and the class members have been injured in their property as a direct result of the above alleged racketeering activity, having lost approximately $172,000 worth of Ether and $186 million respectively from the Nomad Enterprise's illegal money-transmitting business.

***Count Three*: Negligence (Against the Nomad Defendants)**

141. Singh incorporates all prior paragraphs by reference here.

142. The Nomad Defendants, who collectively operate the Nomad Bridge, owed Singh a duty of care to protect his funds from theft because they received those funds for the purpose of transmitting them.

143. The Nomad Defendants breached that duty by failing to establish adequate systems to protect funds.

144. In the alternative or additionally, the Nomad Defendants breached that duty by deploying defective software code in a manner lacking ordinary care or, in the alternative, employing someone who deployed defective software code in the scope of her employment in a manner lacking ordinary care.

145. As a result of the Nomad Defendants' negligence, Singh and the class members lost crypto assets worth hundreds of millions of dollars.

***Count Four*: Conversion (Against Nomad Defendants)**

146. Singh incorporates all prior paragraphs by reference.

147. Singh gave custody of his assets to the Nomad Defendants for the purpose of transmitting those assets from his account at one blockchain to his account at another blockchain.

148. The Nomad Defendants employed someone who introduced malicious code into the Nomad Bridge within the scope of his or her employment with the Nomad Defendants.

149. This person or someone associated with this person used the malicious code in the Nomad Bridge to steal Singh's and the class members' crypto assets.

***Count Five*: Breach of Contract (Against the Nomad Defendants)**

150. Singh incorporates all prior paragraphs by reference.

151. The Nomad Defendants acquired control of Singh's and the class members' crypto assets for the purpose of transferring them across the Nomad Bridge between blockchains.

152. Before the loss or theft of Singh's and the class members' crypto assets, the Nomad Defendants published security-related representations on the Nomad website and in other media, promising to protect users' assets with the highest level of security.

153. Singh and the class members would not have entrusted their crypto assets to the Nomad Defendants if they had known that the Nomad Defendants' security-related representations were false, and that the Nomad Defendants had no way in fact to prevent malicious actors from stealing their assets.

154. In the course of acquiring control over Singh's and class members' crypto assets and publishing security-related representations, the Nomad Defendants entered into express or implied contracts with Singh and the class members under which the Nomad Defendants agreed to protect and secure such crypto assets in exchange for Singh and the class members surrendering them.

155. Singh and the class members fully performed their obligation under their contracts with the Nomad Defendants.

156. The Nomad Defendants failed to perform their obligations under their contracts with the class members.

157. By failing to establish adequate systems to protect Singh's and the class members' assets from theft or loss, the Nomad Defendants breached their contracts with them.

158. As a direct and proximate result of this breach, Singh and the class members have suffered injuries—namely, the loss of hundreds of millions of dollars of crypto assets.

Prayer for Relief

Plaintiff Mannu Singh respectfully requests:

- An order certifying this action as a class action, appointing Singh lead plaintiff, and appointing Gerstein Harrow, Gupta Wessler, and Fairmark as class counsel;
- An award of treble damages under 18 U.S.C. § 1964(c) against all Defendants jointly and severally in the amount of $558,387,258;
- In the alternative, an award of compensatory damages against the Nomad Defendants in the amount of $186,129,086; and
- All other relief the Court deems just and proper.

Respectfully submitted,

SAUL EWING LLP

/s/Marisa R. De Feo
Marisa R. De Feo (# 6778)
Michelle C. Streifthau-Livizos (# 6584)
1201 N. Market Street, Suite 2300
Wilmington, DE 19801
marisa.defeo@saul.com
michelle.streifthau-livizos@saul.com

OF COUNSEL:

Charles Gerstein (*pro hac vice* application forthcoming)
Emily Gerrick*
GERSTEIN HARROW LLP
810 7th Street NE, Suite 301
Washington, DC 20003
charlie@gerstein-harrow.com
(202) 670-4809

Jason Harrow (*pro hac vice* application forthcoming)
GERSTEIN HARROW LLP
3243B S. La Cienega Blvd.,
Los Angeles, CA 90016
jason@gerstein-harrow.com
(323) 744-5293

Neil K. Sawhney (*pro hac vice* application forthcoming)
GUPTA WESSLER PLLC
100 Pine Street, Suite 1250
San Francisco, CA 94111
neil@guptawessler.com
(415) 573-0336

Jamie Crooks (*pro hac vice* application forthcoming)
FAIRMARK PARTNERS LLP
1825 7th Street, NW, #821
Washington, DC 20001
jamie@fairmarklaw.com
(619) 507-4182

** Pro Hac Vice application forthcoming. Admitted to practice in Texas only. Not admitted in the District of Columbia; practice limited pursuant to D.C. App. R. 49(c)(8), with supervision by Charles Gerstein.*

ClassAction.org
