2323016

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Andrew N. Ferguson, Chairman**
Mark R. Meador

In the Matter of

ILLUSORY SYSTEMS, INC.,
a corporation, also d/b/a NOMAD.

DOCKET NO.

COMPLAINT

The Federal Trade Commission, having reason to believe that Illusory Systems, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Illusory Systems, Inc., also doing business as Nomad ("Nomad"), is a Delaware corporation with its principal office or place of business at 331 W. Parish Lane Suite 106-317, Centerville, Utah 84014.

2. Respondent has designed, operated, and advertised a service that allows users to transfer messages and assets, a type of platform commonly known as a "cross-chain bridge."

3. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Business Practices

4. The Nomad Messaging Protocol is a communication protocol that allows developers to build cross-chain applications ("xApps").

5. Beginning in January 2022, Nomad developed and offered for service its own xApp, the Nomad Token Bridge, that used the Nomad Messaging Protocol and that allowed assets to be "bridged."

6. Users generally interacted with the Nomad Token Bridge through a web-based interface. The Nomad Token Bridge was deployed as "smart contracts," programs that are accessible on a network and automatically run when specified conditions are met. The Nomad

Token Bridge executed its smart contracts when a user sent the bridge assets, along with a message indicating where the equivalent value in assets should be sent.

7. The Nomad Token Bridge would then process this message by "locking" the assets from the origin into the bridge. This would mint an equivalent amount of "wrapped" assets on the destination and send the newly minted assets to the specified address on the destination.

8. As discussed further below, in June 2022, in response to a security audit, Nomad introduced new, inadequately tested code for a smart contract that included a significant vulnerability. On August 1, 2022, hackers began to exploit that vulnerability, and, due to Nomad's inadequate security and incident response measures, Nomad could not respond to the attack in time. As a result, virtually all assets in the bridge—worth approximately $186 million—were transferred out. Nomad users lost more than $100 million.

Security Representations

9. Nomad has disseminated or has caused to be disseminated advertisements for the Nomad Cross-Chain Messaging Protocol and Nomad Token Bridge, including but not necessarily limited to the attached Exhibits A through G. These materials contain the following statements:

> A. [Referencing Nomad's network] Powered by Nomad and Connext, users get the best of all worlds:
>
> **High security**, low cost, and fast bridging.
>
> (Exhibit A, www.nomad.xyz) (emphasis added).
>
> B. Nomad is a **security-first** cross-chain messaging protocol
>
> (Exhibit B, www.nomad.xyz) (emphasis added).
>
> C. With $1.5B in bridge hacks happening within the last 12 months, many people, protocols, and DAOs [Decentralized Autonomous Organizations] are looking for an interoperability **solution that prioritizes the safety and security of their funds/cross chain messages**.
>
> This is why we designed Nomad in a way that minimizes the trust assumptions for bridging. ... Nomad's optimistic verification allows any single, honest watcher to prevent fraud via on-chain proofs, and **keep the entire system (and your funds/messages) safe**.
>
> (Exhibit C, https://medium.com/nomad-xyz-blog/nomad-announces-new-cohort-of-investors-to-help-grow-security-first-cross-chain-messaging-solution-d538f955d8c) (underlined emphasis in original; bold emphasis added).

D. Using Nomad, developers can **securely** build cross-chain applications (or xApps) and bridge assets between chains. ...

> We strive to **take advantage of every tool that protects users**. We aim to minimize the probability and impact of security issues.
>
> (Exhibit D, https://medium.com/nomad-xyz-blog/the-nomad-design-philosophy-6fc0eacf3263) (emphasis added).

E. **Security is paramount for Nomad**. ... This means considering financial controls and other common security measures taken in traditional finance.

> (Exhibit E, docs.nomad.xyz/the-nomad-protocol/security) (emphasis added).

F. People want to bridge now, and we need to enable them to do it safely. As such, Nomad is designed around principles that **prioritize safety**, simplicity, and our users.

> (Exhibit F, https://medium.com/nomad-xyz-blog/nomad-raises-22m-seed-round-for-security-first-interoperability-5d6b15c96007) (underline emphasis in original; bold emphasis added).

G. **"We're secure... period"**

> (Exhibit G, https://x.com/nomadxyz_/status/1486804062431547395) (Respondent social media account quoting CEO) (quotes and ellipses in original; emphasis added).

10. These representations were material to users, who stood to lose substantial assets if the bridge were insecure. One third-party analysis noted, for example, that users of the Token Bridge entrusted it with more assets per user than a competitor, which suggested "deep trust in Nomad's security among bridge users," and that Nomad's growth suggested that "Nomad's security appeals are marketable & perceived valuable."

Security Practices

11. Since at least January 2022, despite knowing smart contract exploits can result in the catastrophic loss of all funds and that cross-chain bridges are often a target of sophisticated adversaries, Respondent has failed to engage in reasonable and appropriate security practices. Among other things, Respondent:

A. Contrary to widely-accepted coding practices, failed to implement well-known secure coding practices, such as writing and conducting adequate unit tests prior to pushing code into production. While Nomad stressed the importance of thoroughly testing smart contracts in its marketing, in many instances, it did not adequately test smart contracts, as discussed by Nomad engineers before the exploit. A post-exploit analysis determined that the tests mostly covered "happypath" scenarios, meaning that Nomad only tested whether a smart contract would process messages as valid when sent valid inputs. Nomad did not test whether the smart contract would process certain messages as valid when sent *invalid* inputs, even though invalid inputs were reasonably foreseeable.

B. Contrary to widely-accepted coding practices, failed to have a clear process for receiving and addressing security vulnerability reports, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.

C. Contrary to widely-accepted information management practices, failed to have a Written Information Security Plan ("WISP") and adequate process for incident response. This failure resulted, among other things, in confusion and delay while responding to the exploit.

D. Contrary to widely-accepted information management practices, failed to have adequate staff to address security.

E. Contrary to widely-accepted industry norms and employee recommendations, failed to have sufficient measures, such as automated systems, to detect unusual transactions and patterns of transactions. Thus, instead of learning of a problem promptly through its own systems, the company was first alerted to a suspicious pattern of transactions by a social media user, and lead engineers initially debated whether the screenshots were faked.

F. Contrary to widely-accepted industry norms and employee recommendations, failed to take reasonable measures to implement widely-known technologies that would mitigate critical loss of user funds. For example, the company failed to incorporate "circuit breakers" or a "kill switch" that could immediately cease the functioning of the Nomad Token Bridge in the presence of suspicious transactions.

12. Nomad knew of the dangers of rushing code into production. For example, one possible business partner warned Nomad about the need to be deliberate about upgrades "since upgrades themselves are risky and could lead to unrecoverable funds." Nomad ignored this warning, pushing into production the code that was later exploited.

13. Nomad also failed to hire adequate staff to address security, even though Nomad's leadership knew such staff was necessary to secure its data. Nomad was aware it needed to hire someone "who has deployed smart contracts to production and hardened them." Despite this, Nomad made the Token Bridge available for use before hardening them.

14. Nomad knew of the critical importance of circuit breakers to secure users' assets but failed to deploy them. For example, a Nomad marketing page noted the "absurdity of letting $100M exit in one transaction without any circuit breakers." Similarly, a senior engineer suggested to Nomad's COO and others that Nomad should develop a "set of circuit breakers and the cultural mindset that everyone can and should pull them in the event of suss [suspicious activity]." Despite these acknowledgements, Respondent failed to include any such circuit breakers in Nomad's own technology.

15. Because Nomad failed to implement adequate incident response systems, Nomad did not have an effective way to stop the exploit. Nomad had to rely on an engineer, who was on a plane, to relay code snippets in a chat back and forth with the incident manager on duty. As a result, Nomad was unable to shut down the bridge until after it had been emptied of assets.

16. These security failings were known within Nomad. Months prior to the exploit, an engineer raised concerns to the CEO about code testing and code quality assurance. The engineer pointed out to the CEO that a significant prior vulnerability (predating the code that caused the breakdown at issue in this case) had already made it into production due to a lack of testing. The engineer documented that the rush to deploy and push code into production resulted in a failure to test properly. The engineer further noted that the company needed to conduct quality assurance in the development process and develop a culture of testing and quality assurance.

17. Top level executives were aware of the lack of adequate testing. For example, senior executives knew of an engineer's request to determine "how much of a lift [it] would be to add proper testing."

18. In another instance, a user complained that they were unable to access assets that had been transferred using the Token Bridge. After an internal review revealed that a bug in the web-based interface of the Token Bridge was responsible for the loss of funds, the executives overrode an employee's suggestion to reimburse the user because it would cause more people to make claims. Despite the fact that Nomad had expressly promised its users security, internally, the CEO asserted that Nomad was "putting out a free to use interface to a protocol that may have bugs / issues," and the COO agreed with not reimbursing the user because "there are no guarantees of safety."

19. One engineer found that 36 "watcher" wallets—a key part of Nomad's security model—were running low on funds and needed manual adjustment. He reported to management that the process should have been automated. He observed that the issue was "a bit disappointing to see ... as we're supposed to be a security first company." He further warned that "continually punting is how we eventually end up getting rugged without noticing an error."[1]

Breach of Security

20. As a result of the failures described in paragraph 11, in August 2022, hackers exploited a vulnerability in the Nomad Token Bridge and users of the bridge lost more than $100 million worth of assets.

21. The vulnerability was caused by the interaction between a pre-existing entry in the initialization table of a smart contract and a June 21, 2022 code update.

22. The result of the interaction had the effect of causing the smart contract to fail to authenticate messages properly and allowed for any message to be executed so long as the messages had not already been processed. Users could therefore extract assets from the Token Bridge without authorization.

[1] "Getting rugged" is slang for "getting the rug pulled out from under us."

23. This vulnerability was first exploited on August 1, 2022. As the method of attack became known, hundreds of near-identical transactions were sent to the bridge. Within hours, these transactions drained the bridge of assets worth approximately $186 million that had been deposited by users.

24. After learning of the breach, Respondent notified law enforcement and worked with experts to track and identify the hackers. Respondent also requested that hackers—including "white hat" hackers who had exploited the vulnerability to secure assets before the other hackers could drain it all from the bridge for malicious reasons—return funds to Nomad so they could be returned to users. "White hat" hackers did return funds, and the company was able to recover some $37,500,000 in nominal asset value. Nomad has partnered with multiple third parties to return recovered funds to users.

CONSUMER INJURY

25. Consumers have suffered substantial injury as a result of Respondent's violations of the FTC Act. As described in paragraphs 23 and 24, consumers lost over one hundred million dollars in value due to Nomad's violations.

26. Respondent could have prevented or mitigated its failures through readily available and relatively low-cost measures.

Count 1
Unfair Security Practices

27. As described in Paragraphs 11-19, Respondent's failure to employ reasonable and appropriate software development practices caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count 2
Security Misrepresentations

28. As described in Paragraph 9, Respondent has represented, directly or indirectly, expressly or by implication, that it implemented secure software development practices.

29. In fact, as set forth in Paragraph 11, Respondent did not implement secure software development practices. Therefore, the representation set forth in Paragraph 28 is false or misleading.

VIOLATIONS OF SECTION 5

30. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ___ day of ________, 20__, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL: