

## **Analysis of Proposed Consent Order to Aid Public Comment In the Matter of Illusory Systems, Inc., File No. 2323016**

The Federal Trade Commission (“Commission”) has accepted, subject to final approval, an agreement containing a consent order from Illusory Systems, Inc., doing business as Nomad (“Respondent”).

The proposed consent order (“proposed order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

This matter involves Respondent’s software development practices. Respondent operated an online service, a token bridge, through which consumers could transfer assets to peers.

The proposed complaint alleges that Respondent claimed to keep users’ assets secure, but in fact failed to implement reasonably secure software development practices. For example, the proposed complaint alleges that Respondent failed to: conduct adequate unit tests, implement a process for receiving and addressing third-party security vulnerability reports, have a Written Information Security Plan, and implement widely-known technologies that would mitigate critical loss of user funds. The proposed complaint alleges that as a result of Respondent’s failures, in August 2022, hackers exploited a significant vulnerability in the token bridge and took virtually all of its assets – worth approximately \$186 million. Even after Respondent recovered some assets and returned them to users, users of the bridge were left with losses that exceeded \$100 million worth of assets.

The proposed complaint alleges that Respondent violated Section 5(a) of the FTC Act by: (1) failing to employ reasonable and appropriate software development practices; and (2) misrepresenting that it implemented secure software development practices. The proposed order contains provisions designed to prevent Respondent from engaging in the same or similar acts or practices in the future.

**Part I** prohibits Respondent from misrepresenting (1) the extent to which Respondent implements reasonable and appropriate software development practices; and (2) the extent to which it secures consumers’ financial assets.

**Part II** requires Respondent to establish and implement, and thereafter maintain, a comprehensive information security program (“Security Program”) that protects the consumers’ financial assets.

**Part III** requires Respondent to obtain initial and biennial data security assessments for ten years.

**Part IV** requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessment required by Part III.

**Part V** requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

**Part VI** requires Respondent to return recovered assets to users and to submit a report at the conclusion of the program summarizing its compliance.

**Part VII** requires Respondent to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which Respondent has delivered a copy of the order.

**Part VIII** requires Respondent to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations.

**Part IX** contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and all records necessary to demonstrate compliance with the order.

**Part X** contains other requirements related to the Commission's monitoring of Respondent's order compliance.

**Part XI** provides the effective dates of the order, including that, with exceptions, the order will terminate in 10 years.

The purpose of this analysis is to facilitate public comment on the order, and it is not intended to constitute an official interpretation of the complaint or order, or to modify the order's terms in any way.