persons providing insurance, investment companies, and investment advisers) relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer.

The Interagency Guidelines Establishing Information Security Standards, 12 CFR part 30, appendix B (Security Guidelines), which implement section 501(b), require each entity supervised by the OCC (supervised institution) to consider and adopt a response program, as appropriate, that specifies actions to be taken when the supervised institution suspects or detects that unauthorized individuals have gained access to customer information systems.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Breach Notice Guidance),[1] which interprets the Security Guidelines, states that, at a minimum, a supervised institution's response program should contain procedures for:

(1) Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;

(2) Notifying its primary Federal regulator as soon as possible when the supervised institution becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information;

(3) Notifying appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, consistent with the OCC's Suspicious Activity Report regulations;

(4) Taking appropriate steps to contain and control the incident in an effort to prevent further unauthorized access to, or use of, customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and

(5) Notifying customers when warranted.

The Breach Notice Guidance states that, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that the misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.

Estimated Burden:

Estimated Frequency of Response: On occasion.

Estimated Number of Respondents: 30.

Estimated Total Annual Burden: 1,080 hours.

Comments submitted in response to this notice will be summarized and included in the request for OMB approval. All comments will become a matter of public record. Comments are invited on:

(a) Whether the collection of information is necessary for the proper performance of the functions of the OCC, including whether the information has practical utility;

(b) The accuracy of the OCC's estimate of the burden of the collection of information;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

Patrick T. Tierney,

Assistant Director, Office of the Comptroller of the Currency.

[FR Doc. 2025–09963 Filed 6–2–25; 8:45 am]

BILLING CODE 4810–33–P

[1] 12 CFR part 30, appendix B, supplement A.

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: This action was issued on May 29, 2025. See **SUPPLEMENTARY INFORMATION** for relevant dates.

FOR FURTHER INFORMATION CONTACT: OFAC: Associate Director for Global Targeting, 202–622–2420; Assistant Director for Sanctions Compliance, 202–622–2490; or *https://ofac.treasury.gov/contact-ofac.*

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website: *https://ofac.treasury.gov.*

Notice of OFAC Action

On May 29, 2025, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are blocked under the relevant sanctions authority listed below.

BILLING CODE 4810–AL–P

Individual:

1. LIU, Lizhi (Chinese Simplified: 刘理志) (a.k.a. "ENJOYGANZHOU"; a.k.a. "LIU, Steve"; a.k.a. "LIU, Steven"; a.k.a. "NICE LIZHI"; a.k.a. "NICELIZHI"; a.k.a. "XXL4"), No. 2 Shaguo Group, Yangmei Village, Huangjin Ridge, Zhanggong District, Ganzhou, Jiangxi, China; Lianhang Road, No. 1698, 5 Building, Pujiang Town, Minxing District, Shanghai, China; Lulian Road, 100 Alley, No. 5, Room 1202, Pujiang Town, Minxing District, Shanghai, China; Puxinggong Road, 9688, Alley No. 5, Haiwan Town, Fengxian District, Shanghai, China; DOB 13 Nov 1984; POB Zhanggong District, Ganzhou, Jiangxi, China; nationality China; Gender Male; National ID No. 360702198411133 73X (China) (individual) [CYBER3] (Linked To: FUNNULL TECHNOLOGY INC).

   Designated pursuant to section (1)(a)(iii)(D) of Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 FR 18077, 3 CFR, 2015 Comp., p. 297, as amended by Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," 82 FR 1, 3 CFR, 2016 Comp., p. 659, and as further amended by Executive Order 14144 of January 16, 2025, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," 90 FR 6755, CFR (E.O. 13694, as further amended), for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, FUNNULL TECHNOLOGY INC, a person whose property and interests in property are blocked pursuant to this order.

Entity:

1. FUNNULL TECHNOLOGY INC (a.k.a. FANG NENG CDN (Chinese Simplified: 方能CDN); a.k.a. FUNNULL; a.k.a. FUNNULL CDN; a.k.a. FUNNULL INC; a.k.a. FUNNULL LLC), 3rd Avenue and 30th Street, 14th Floor, C6 Road, Purok 5, Net Cube Center, E Square Zone, Lower Bicutan, Fourth District, Taguig City, National Capital Region 1632, Philippines; China; Website funnull.io; alt. Website funnull.com; alt. Website funnull.app; alt. Website funnull.buzz; Digital Currency Address - ETH 0xd5ED34b52AC4ab84d8FA8A231a3218bbF01Ed510; Organization Established Date 07 Sep 2021; Organization Type: Other information technology and computer service activities; Digital Currency Address - TRX TNmRfnSUXZoWWzxcDDbf95eGQYXt1mJDt8; Registration Number 2021090024665-00 (Philippines) [CYBER3].

   Designated pursuant to section (1)(a)(iii)(C) of E.O. 13694, as further amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a threat to the national security, foreign policy, or economic health or financial stability of the United States, and that have the purpose of or involve causing a misappropriation of funds or economic resources, intellectual property, proprietary or business confidential information, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

Lisa M. Palluconi,

Acting Director, Office of Foreign Assets Control.

[FR Doc. 2025–10055 Filed 6–2–25; 8:45 am]

BILLING CODE 4810–AL–C