

中華民國證券投資信託暨顧問商業同業公會 函

地址：10459台北市中山區長春路145號3樓
承辦人：曾珮琪
電話：(02)2581-7288#205
傳真：(02)2581-7388
電子信箱：Mickey.Tseng@sitca.org.tw

(郵遞區號)

(地址)

受文者：

發文日期：中華民國111年8月25日

發文字號：中信顧字第1110052617號

速別：普通件

密等及解密條件或保密期限：

附件：如文

主旨：函轉金融監督管理委員會檢送有關駐美國代表處經濟組
111年8月8日經美字第1110000833號函知美國財政部發布
制裁虛擬貨幣混合器Tornado Cash一案，請查照。

說明：

- 一、依金融監督管理委員會111年8月24日金管證券字第
1110354787號函辦理。
- 二、請各會員公司如發現疑似洗錢或資恐交易，請向法務部
調查局申報及注意該等交易之風險。

正本：本公會各投信會員公司、本公會各投顧會員公司

副本：

理事長 **劉宗聖**

檔 號：

保存年限：

金融監督管理委員會 函

機關地址：22041新北市板橋區縣民大道2
段7號18樓

承辦人：鄭先生
電話：02-27747266

受文者：中華民國證券投資信託暨顧問商業同業公會（代表人
劉宗聖先生）

發文日期：中華民國111年8月24日

發文字號：金管證券字第1110354787號

速別：普通件

密等及解密條件或保密期限：

附件：如文(附件1 111UJ05759_1_24160843079.pdf、附件2 111UJ05759_2_
24160843079.pdf)

主旨：有關美國財政部發布制裁虛擬貨幣混合器Tornado Cash一
案，請依說明二辦理，請查照。

說明：

- 一、依據駐美國代表處經濟組111年8月8日經美字第
1110000833號函辦理。
- 二、本案請轉知所屬會員，如發現疑似洗錢或資恐交易，請
向法務部調查局申報及注意該等交易之風險，併請副本
收文者配合辦理。
- 三、檢送駐美國代表處經濟組111年8月8日經美字第
1110000833號函影本暨附件各一份。

正本：中華民國證券商業同業公會（代表人陳俊宏先生）、中華民國期貨業商業同業
公會（代表人陳佩君先生）、中華民國證券投資信託暨顧問商業同業公會（代
表人劉宗聖先生）、中華民國會計師公會全國聯合會（代表人黃奕睿先生）

副本：臺灣證券交易所股份有限公司（代表人林修銘先生）、財團法人中華民國證券
櫃檯買賣中心（代表人陳永誠先生）、臺灣期貨交易所股份有限公司（代表人
吳自心先生）、臺灣集中保管結算所股份有限公司（代表人朱漢強先生）、元
大證券金融股份有限公司（代表人龔紹興先生）(均含附件)

111/08/24
16:21:13

中華民國證券投資信託暨顧問商業同業公會（代表



檔 號：
保存年限：

駐美國代表處經濟組 函

地址：4301 Connecticut Ave., N.W. Suite 420, Washington, D.C. 20008 USA

承辦人：侯文萃
電話：202-686-6400#5712
傳真：202-363-6294
Email：wphou@moea.gov.tw

受文者：金融監督管理委員會

發文日期：中華民國111年8月8日
發文字號：經美字第1110000833號
速別：普通件
密等及解密條件或保密期限：
附件：如文(經美1110000833_Attach1.pdf)

主旨：陳報美財政部制裁虛擬貨幣混合器Tornado Cash事，敬請查參。

說明：

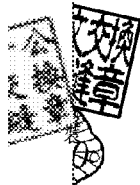
- 一、美財政部本(8)月8日發布新聞稿略以，該部外國資產管制辦公室(OFAC)依據第13694號行政命令將虛擬貨幣混合器Tornado Cash列入「管制名單」(SDN List)予以制裁；該虛擬貨幣混合器可被用於網路犯罪洗錢，自2019年Tornado Cash成立以來，進行超過70億美元之虛擬貨幣洗錢，包括北韓國有駭客組織 Lazarus Group竊取之4.55億美元。
- 二、前述被制裁對象在美或由美國人(包括自然人及法人)營運之資產將被凍結，且必須向OFAC報告；依據相關法規，原則禁止美國自然人/法人或是在美境內參與涉及該等被制裁者之資產交易，包括對該等被制裁對象提供捐款、資金、貨品或服務等。

三、檢送前述新聞資料如附件，併請查參。

正本：經濟部國際貿易局

副本：金融監督管理委員會(含附件)

2022/08/11
10:46:06



訂



線

U.S. DEPARTMENT OF THE TREASURY

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash



August 8, 2022

WASHINGTON – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash, which has been used to launder more than \$7 billion worth of virtual currency since its creation in 2019. This includes over \$455 million stolen by the Lazarus Group, a Democratic People’s Republic of Korea (DPRK) state-sponsored hacking group that was sanctioned by the U.S. in 2019, in the largest known virtual currency heist to date. Tornado Cash was subsequently used to launder more than \$96 million of malicious cyber actors’ funds derived from the June 24, 2022 Harmony Bridge Heist, and at least \$7.8 million from the August 2, 2022 Nomad Heist. Today’s action is being taken pursuant to Executive Order (E.O.) 13694, as amended, and follows OFAC’s May 6, 2022 designation of virtual currency mixer Blender.io (Blender).

“Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.

“Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them.”

Treasury has worked to expose components of the virtual currency ecosystem, like Tornado Cash and Blender.io, that cybercriminals use to obfuscate the proceeds from illicit cyber activity and other crimes. While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, fraud, and other cybercrimes. Treasury continues to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as foreign partners, to expose, disrupt, and hold accountable perpetrators and persons that enable criminals to profit from cybercrime and other illicit activity. For example, in 2020, Treasury’s Financial Crimes Enforcement Network

(FinCEN) assessed a \$60 million civil money penalty against the owner and operator of a virtual currency mixer for violations of the Bank Secrecy Act (BSA) and its implementing regulations.

MIXER: TORNADO CASH

Tornado Cash (Tornado) is a virtual currency mixer that operates on the Ethereum blockchain and indiscriminately facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin. Tornado receives a variety of transactions and mixes them together before transmitting them to their individual recipients. While the purported purpose is to increase privacy, mixers like Tornado are commonly used by illicit actors to launder funds, especially those stolen during significant heists.

Tornado is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

ILLICIT FINANCE RISKS

Virtual currency mixers that assist criminals are a threat to U.S. national security. Treasury will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financing risks in the virtual currency ecosystem.

Criminals have increased their use of anonymity-enhancing technologies, including mixers, to help hide the movement or origin of funds. Additional information on illicit financing risks associated with mixers and other anonymity-enhancing technologies in the virtual asset ecosystem can be found in the 2022 National Money Laundering Risk Assessment.

Those in the virtual currency industry play a critical role in complying with their Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and sanctions obligations to

prevent sanctioned persons and other illicit actors from exploiting virtual currency to undermine U.S. foreign policy and national security interests. As part of that effort, the industry should take a risk-based approach to assess the risk associated with different virtual currency services, implement measures to mitigate risks, and address the challenges anonymizing features can present to compliance with AML/CFT obligations. As today's action demonstrates, mixers should in general be considered as high-risk by virtual currency firms, which should only process transactions if they have appropriate controls in place to prevent mixers from being used to launder illicit proceeds.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the entity above, Tornado Cash, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 [here](#). For detailed information on the process to submit a request for removal from an OFAC sanctions list, [click here](#).

For identifying information on the entity sanctioned today, as well as associated virtual wallet addresses, [click here](#).

To report a cyber-crime, contact the Federal Bureau of Investigation's Internet Crime Complaint Center [here](#).

For the U.S. government's 2020 DPRK Cyber Threat Advisory, [click here](#).

For information on complying with virtual currency sanctions, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry [here](#) and OFAC's FAQs on virtual currency [here](#).

###

