

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：林采蓉
電話：(02)2581-7288#206
傳真：(02)2581-7388
電子信箱：Tsaijung.Lin@sitca.org.tw

(郵遞區號)

(地址)

受文者：

發文日期：中華民國107年12月13日
發文字號：中信顧字第1070053107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美國財政部107年11月28日公告新增2名個人於制裁名單(SDN list)一案，如發現疑似洗錢或資恐交易，請向法務部調查局申報，並注意該等交易風險，請查照。

說明：依金融監督管理委員會107年12月7日金管證券字第10703458481號函辦理。

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 張錫

裝

訂

線

檔 號：

保存年限：

金融監督管理委員會 函

機關地址：新北市板橋區縣民大道二段7號
18樓

聯絡人：鄭先生

聯絡電話：(02) 27747266

傳 真：(02) 87734411

受文者：中華民國證券投資信託暨顧問商業同業公會

發文日期：中華民國107年12月7日

發文字號：金管證券字第10703458481號

速別：普通件

密等及解密條件或保密期限：

附件：如主旨(第一件 A45020000DORGUNIT107120703458481A2B345848.PDF)

主旨：有關美國財政部107年11月28日公告新增2名個人於制裁名單(SDN list)一案，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，並注意該等交易風險，請查照。

說明：

- 一、依據駐美國代表處經濟組107年11月28日經美字第1070001429號函副本辦理。
- 二、檢附駐美國代表處經濟組函文及美國財政部107年11月28日公告影本各一份。

正本：中華民國證券商業同業公會、中華民國期貨業商業同業公會、中華民國證券投資信託暨顧問商業同業公會、中華民國會計師公會全國聯合會(均含附件)

副本：臺灣證券交易所股份有限公司、財團法人中華民國證券櫃檯買賣中心、臺灣期貨交易所股份有限公司、臺灣集中保管結算所股份有限公司、金融監督管理委員會證券期貨局(證券發行組、投信投顧組、會計審計組、期貨管理組)

107/12/07
11:49:09

授權單位主管決行並鈐印



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, DC 20008

承辦人：趙堅集

電話：(202)686-6400#112

傳真：(202)363-6294

Email：ccchao@moea.gov.tw

受文者：金融監督管理委員會

發文日期：中華民國107年11月28日

發文字號：經美字第1070001429號

速別：普通件

密等及解密條件或保密期限：

附件：如文(1070001429_Attach1.docx、1070001429_Attach2.pdf)

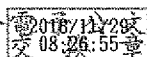
主旨：陳報美國財政部公告新增2名個人於制裁名單(SDN list)事，敬請查照。

說明：

- 一、美財政部於本(2018)年11月28日發布新聞稿略以，該部外國資產管制局(OFAC)以為使用SamSam勒索軟體之駭客，將其所獲比特幣贖金轉換成伊朗里拉為由，將Ali Khorashadizadeh與Mohammad Ghorbaniyan等兩名伊朗人納入制裁名單，並公布渠等使用之虛擬貨幣地址，實施第二級制裁，凍結其於美國境內之資產與交易。
- 二、檢附上述財政部新聞稿如附件，併請卓參。


正本：經濟部國際貿易局

副本：金融監督管理委員會





PRESS RELEASES



Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses

November 28, 2018

WASHINGTON – The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) took action today against two Iran-based individuals, **Ali Khorashadizadeh** and **Mohammad Ghorbaniyan**, who helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims. Also today, OFAC identified two digital currency addresses associated with these two financial facilitators. Over 7,000 transactions in bitcoin, worth millions of U.S. dollars, have processed through these two addresses - some of which involved SamSam ransomware derived bitcoin. In a related action, the U.S. Department of Justice today indicted two Iranian criminal actors for infecting numerous data networks with SamSam ransomware in the United States, United Kingdom, and Canada since 2015.

“Treasury is targeting digital currency exchangers who have enabled Iranian cyber actors to profit from extorting digital ransom payments from their victims. As Iran becomes increasingly isolated and desperate for access to U.S. dollars, it is vital that virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services harden their networks against these illicit schemes,” said Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker. “We are publishing digital currency addresses to identify illicit actors operating in the digital currency space. Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives.”

Today’s action focuses on a ransomware scheme known as “SamSam” that has victimized numerous corporations, hospitals, universities, and government agencies and held over 200 known victims’ data hostage for financial gain. To execute the SamSam ransomware attack, cyber actors exploit computer network vulnerabilities to gain access and copy the SamSam ransomware into the

network. Once in the network, these cyber actors use the SamSam ransomware to gain administrator rights that allow them to take control of a victim's servers and files, without the victim's authorization. The cyber actors then demand a ransom be paid in bitcoin in order for a victim to regain access and control of its own network.

Central to the SamSam ransomware scheme's success were **Khorashadizadeh** and **Ghorbaniyan**, who helped the cyber actors exchange digital currency derived from ransom payments into Iranian rial and also deposited the rial into Iranian banks. To help convert the digital currency ransom payments into rial, **Khorashadizadeh** and **Ghorbaniyan** used the following two digital currency addresses: 149w62rY42aZBox8fGcmqNsXUzSStKeq8C and 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V. Since 2013, **Khorashadizadeh** and **Ghorbaniyan** have used these two digital currency addresses to process over 7,000 transactions, to interact with over 40 exchangers—including some US-based exchangers—and to send approximately 6,000 bitcoin worth millions of USD, some of which involved bitcoin derived from SamSam ransomware.

While OFAC routinely provides identifiers for designated persons, today's action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses. As a result of today's action, persons that engage in transactions with **Khorashadizadeh** and **Ghorbaniyan** could be subject to secondary sanctions. Regardless of whether a transaction is denominated in a digital currency or traditional fiat currency, OFAC compliance obligations are the same. See OFAC's updated FAQ's for additional information on compliance requirements for digital currencies.

OFAC designated Iran-based **Khorashadizadeh** and **Ghorbaniyan** pursuant to Executive Order 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, the SamSam ransomware attacks. The SamSam ransomware attacks are 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 significant threat to the national security, foreign policy, or economic health or financial stability of the United States that have the purpose or effect of harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector, causing a significant disruption to the availability of a computer or network of computers, and 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.

As a result of today's action, all property and interests in property of the designated persons that are in the possession or control of U.S. persons or within or transiting the United States are blocked, and U.S. persons generally are prohibited from dealing with them.

Today's action marks the fourth round of U.S. sanctions targeting the Iranian regime this month. Under this Administration, in less than two years, OFAC has sanctioned more than 900 individuals, entities, aircraft, and vessels, including for a range of activities related to Iran's support for terrorism, ballistic missile program, weapons proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses. This marks the highest-ever level of U.S. economic pressure targeting the Iranian regime. This sanctions pressure campaign is designed to blunt the broad spectrum of the Iranian regime's malign activities and compel the regime to change its behavior.

OFAC closely coordinated its action with the Department of Justice and the Federal Bureau of Investigation, which released details regarding its law enforcement action against the two Iranian criminal cyber actors.

Identifying information on the entities designated today.





2018/11/28

Cyber-related Designations; Publication of New Cyber-related FAQs

U.S. DEPARTMENT OF THE TREASURY

Resource Center

Cyber-related Designations; Publication of New Cyber-related FAQs

11/28/2018

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing two new Frequently Asked Questions (FAQs) to provide guidance on digital currency.

In addition, the following changes to the Specially Designated Nationals List occurred today:

The following individuals have been added to OFAC's SDN List:

GHORBANIYAN, Mohammad (a.k.a. GHORBANIYAN, Mohammad; a.k.a. "EnExchanger"; a.k.a. "Ensaniyat"; a.k.a. "Ensaniyat_Exchangeer"), Iran; DOB 05/11/1987; POB Tehran, Iran; nationality Iran; Website www.enexchanger.com; Email Address EnExchanger@gmail.com; alt. Email Address Ensaniyat1365@gmail.com; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male; Digital Currency Address - XBT 6nZPMsnmpdK2Rv9KQNfMurTXinscVro9V; Identification Number 008-046347-9 (Iran); Birth Certificate Number 32270 (Iran) (individual) [CYBER2].

KHAYYER SHADIZADEH, Ali (a.k.a. "Iranvisacart"; a.k.a. "Mastercartaria"), Iran; DOB 21 Sep 1979; POB Tehran, Iran; nationality Iran; Email Address iranvisacart@yahoo.com; alt. Email Address mastercartaria@yahoo.com; alt. Email Address alikhorashadi@yahoo.com; alt. Email Address toppglasses@gmail.com; alt. Email Address iranian_boy5@yahoo.com; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male; Digital Currency Address - XBT 149w62rY42aZBox8fGcmqNsXUzSSiKeq8C; Passport T14553558 (Iran) issued 28 Oct 2008 expires 29 Oct 2013 (individual) [CYBER2].

