

檔 號：

保存年限：

# 金融監督管理委員會保險局 函

地址：新北市板橋區縣民大道二段7號17樓

聯絡方式：吳韋村 02-8968-0899#0714



受文者：中華民國人壽保險商業同業公會（代表人黃調貴先生）

發文日期：中華民國107年10月31日

發文字號：保局(綜)字第10704964301號

速別：普通件

密等及解密條件或保密期限：

附件：如說明(107S408816\_1\_311511599811.pdf、107S408816\_2\_311511599811.pdf、107S408816\_3\_311511599811.pdf、107S408816\_4\_311511599811.pdf、107S408816\_5\_311511599811.pdf)

主旨：檢送美國財政部發布伊朗規避制裁之諮詢意見等相關資訊如附件，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：依據本會107年10月29日金管銀法字第10701186560號函（副本）轉法務部調查局107年10月19日調錢貳字第10735568140號函及駐美國代表處經濟組107年10月11日經美字第1070001243號函副本辦理。檢送來函及附件影本各一份供參。

正本：台灣人壽保險股份有限公司(代表人黃思國先生)、國泰人壽保險股份有限公司(代表人黃調貴先生)、中國人壽保險股份有限公司(代表人王銘陽先生)、南山人壽保險股份有限公司(代表人杜英宗先生)、新光人壽保險股份有限公司(代表人吳東進先生)、富邦人壽保險股份有限公司(代表人蔡明興先生)、三商美邦人壽保險股份有限公司(代表人陳翔玠先生)、全球人壽保險股份有限公司(代表人彭騰德先生)、臺銀人壽保險股份有限公司(代表人劉玉枝女士)、中華郵政股份有限公司(代表人魏健宏先生)、第一金人壽保險股份有限公司、保德信國際人壽保險股份有限公司(代表人葛納森先生)、安聯人壽保險股份有限公司(代表人薛傳睿先生)、保誠人壽保險股份有限公司(代表人劉添先生)、國際康健人壽保險股份有限公司(代表人朱立明先生)、合作金庫人壽保險股份有限公司(代表人杜振遠先生)、元大人壽保險股份有限公司(代表人江朝國先生)、宏泰人壽保險股份有限公司(代表人魯奐毅先生)、遠雄人壽保險事業股份有限公司(代表人孟嘉仁先生)、英屬百慕達商友邦人壽保險股份有限公司台灣分公司(代表人侯文成先生)、英屬百慕達商安達人壽保險股份有限公司台灣分公司、法商法國巴黎人壽保險股份有限公司台灣分公司(代表人戴朝暉先生)、英屬曼島商蘇黎世國際人壽保險股份有限公司台灣分公司、臺灣產物保險股份有限公司(代表人李泰宏先生)、兆豐產物保險股份有限公司(代表人梁正德先生)、富邦產物保險股份有限公司(代表人陳燦煌



裝



訂

線

先生)、和泰產物保險股份有限公司(代表人鄭林經先生)、泰安產物保險股份有限公司(代表人李松季先生)、明台產物保險股份有限公司(代表人熊谷真樹先生)、南山產物保險股份有限公司(代表人陳棠先生)、第一產物保險股份有限公司(代表人李正漢先生)、旺旺友聯產物保險股份有限公司(代表人洪吉雄先生)、新光產物保險股份有限公司(代表人吳昕紘先生)、華南產物保險股份有限公司(代表人吳崇權先生)、國泰世紀產物保險股份有限公司(代表人蔡鎮球先生)、新安東京海上產物保險股份有限公司(代表人陳忠鏗先生)、台壽保產物保險股份有限公司(代表人林欽森先生)、中央再保險股份有限公司(代表人楊誠對先生)、美商安達產物保險股份有限公司台灣分公司(代表人曾增成先生)、香港商亞洲保險有限公司台灣分公司(代表人宋安樂先生)、法商法國巴黎產物保險股份有限公司台灣分公司(代表人王瑜華女士)、法商科法斯產物保險股份有限公司台灣分公司(代表人張育立先生)、德商科隆再保險股份有限公司台灣分公司(代表人曾蕙芬女士)、英屬百慕達商美國再保險股份有限公司台灣分公司(代表人蔡佩君女士)、新加坡商美國國際產物保險股份有限公司台灣分公司(代表人林建忠先生)、比利時商裕利安宜產物保險股份有限公司台灣分公司(代表人郭駿家先生)

副本：中華民國產物保險商業同業公會(代表人陳燦煌先生)、中華民國人壽保險商業同業公會(代表人黃調貴先生)(以上含附件)、本局綜合監理組

2018/11/02  
09:52:47

## 金融監督管理委員會 函

地址：新北市板橋區縣民大道2段7號18樓  
承辦人：高士傑  
電 話：(02)89689629  
傳 真：(02)89691366

受文者：本會保險局

發文日期：中華民國107年10月29日  
發文字號：金管銀法字第10701186560號  
速別：普通件

密等及解密條件或保密期限：

附件：如文(107B104633\_1\_291040459972.pdf、107B104633\_2\_291040459972.pdf、107B104633\_3\_291040459972.pdf、107B104633\_4\_291040459972.pdf)

主旨：有關美國財政部發布伊朗規避制裁之諮詢意見一案，請轉知貴會(社)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、依據法務部調查局107年10月19日調錢貳字第10735568140號函及駐美國代表處經濟組107年10月11日經美字第1070001243號函副本辦理(檢附上二函暨附件一份)。
- 二、旨揭諮詢意見旨在協助美國金融機構(包括銀行、虛擬貨幣管理者與交換者、貴金屬與貴重物品之交易商等)獲悉伊朗所採之違法規避行為，以及協助外國金融機構瞭解其利用美國金融體系進行通匯業務之注意義務、避免制裁風險、執行防制洗錢與打擊資恐等。
- 三、上開諮詢意見指出伊朗規避美國制裁之行為態樣，包括：利用伊朗央行官員個人帳戶或外匯交易所，進行資恐之金流、採購偽造強勢貨品之設備及發展洲際彈道飛彈之軍民兩用設備、利用空殼公司採購相關民航設備、透過船運公司提供偽造文件或變更船籍等方式以獲取收益等，相關例



示行為態樣達21種，該等行為態樣均屬於警訊(red flags)  
)，可協助金融機構作為辨識可疑活動之參考。

正本：中華民國銀行商業同業公會全國聯合會（代表人呂桔誠先生）、有限責任中華民國信用合作社聯合社（代表人麥勝剛先生）、中華民國信託業商業同業公會（代表人雷仲達先生）、中華民國票券金融商業同業公會（代表人楊豐彥先生）、台北市租賃商業同業公會（代表人陳鳳龍先生）

副本：本會證券期貨局(併請轉知所屬相關公會)、保險局(併請轉知所屬相關公會)、檢查局(均含附件)

2018/10/29  
交 11:48:57 章

授權單位主管決行並鈐印



訂



線

檔 號：

保存年限：

## 法務部調查局 函

地址：23149新北市新店區中華路74號

承辦人：徐慶隆

電話：02-29112241#6225

傳真：02-29131280

電子信箱：m37013@mjib.gov.tw

受文者：金融監督管理委員會

發文日期：中華民國107年10月19日

發文字號：調錢貳字第10735568140號

速別：普通件

密等及解密條件或保密期限：

附件：如文(A11010000F\_10735568140A0C\_ATTCH1.pdf、A11010000F\_10735568140A0C\_ATTCH2.pdf)

主旨：檢送美國金融情報中心FinCEN提供之伊朗濫用金融系統參考資料（advisory），惠請參處。

說明：

- 一、日前美國金融情報中心FinCEN提供伊朗濫用金融系統之新聞稿（附件一）暨參考資料（附件二），期能協助與美國金融機構具通匯銀行關係（correspondent banking relationship）之我國金融機構偵測相關可疑金融活動。
- 二、上述參考資料（advisory）列舉伊朗逃避制裁的策略、交易態樣、紅旗指標等。

正本：金融監督管理委員會

副本：

局長 呂文忠

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10月11日

發文字號：經美字第1070001243號

速別：普通件

密等及解密條件或保密期限：

附件：如文(1070001243\_Attach1.docx、1070001243\_Attach2.pdf)

主旨：陳報美國財政部發布伊朗規避制裁之諮詢意見事，敬請查照。

說明：

一、本組本(107)年10月9日經美字第1070001236號函諒達。

二、美財政部金融犯罪執法網絡(Financial Crimes Enforcement Network, FinCEN)於本10月11日就伊朗企圖利用金融體系，以規避制裁之違法行為，發布諮詢意見(Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System)

略以：

(一)本諮詢意見在協助美國金融機構(包括銀行、虛擬貨幣管理者與交換者、貴金屬與貴重物品之交易商等)獲悉伊朗所採之違法規避行為，以及協助外國金融機構瞭解其利用美國金融體系進行通匯業務之注意義務、避免制裁風險、執行防制洗錢與打擊資恐等。

(二)上述諮詢意見指出，伊朗規避行為態樣包括利用伊朗央



行官員個人帳戶或外匯交易所，進行資恐之金流、採購偽造強勢貨品之設備及發展洲際彈道飛彈之軍民兩用設備、利用空殼公司採購相關民航設備、透過船運公司提供偽造文件或變更船籍等方式以獲取收益等，相關例示行為之態樣多達21種。該等行為態樣，均屬於警訊(red flags)金融機構應作為發現或指認可疑行為之參考，並進行進一步調查。

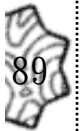
三、檢附美財政部新聞稿及FinCEN諮詢意見如附件，併請卓參

。

正本：經濟部國際貿易局

副本：金融監督管理委員會

2018/10/12  
09:03:21  
電子公文  
交換章



## PRESS RELEASES

# FinCEN Issues Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System

5811

October 11, 2018

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) issued an [advisory](#) today to help financial institutions better detect and report potentially illicit transactions related to the Islamic Republic of Iran. The [advisory](#) is also intended to help foreign financial institutions better understand the obligations of their U.S. correspondents, to avoid exposure to U.S. sanctions, and to address the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) risks that Iranian activity poses to the international financial system. The advisory provides information on the threats the Iranian regime poses to the U.S. financial system as well as to institutions that have correspondent banking relationships with U.S. financial institutions, describes deceptive financial strategies that the Iranian regime uses to evade sanctions, and provides red flag indicators related to specific malign activities and typologies.

“This advisory lays out in great detail the extent to which the Iranian regime uses deceptive practices, including front companies, fraudulent documents, exchange houses, seemingly legitimate businesses and government officials, to generate illicit revenues and finance their malign activities. Iran’s deceptive practices have been orchestrated not only by elements of their government such as the IRGC-Qods Force, but also by Central Bank of Iran officials who were at the highest levels. Any country that allows its Central Bank to be involved in deception in support of terrorism requires the highest levels of scrutiny, particularly when the country itself is the world’s largest state sponsor of terrorism,” said Sigal Mandelker, Under Secretary of the Treasury for Terrorism and Financial Intelligence. “Governments, financial institutions of all types around the world, and other companies need to be on high alert to the types of schemes described in this advisory. More than that, as we expect Iran to continue to attempt to engage in wide scale sanctions evasion while simultaneously using its resources to fund a broad array of malign activity, financial institutions should continue to sophisticate their compliance programs to keep these actors from exploiting them.”



On June 5, 2018, Under Secretary Mandelker delivered [extensive remarks](#) on the surreptitious means by which the Iranian regime finances itself.

“Crucial insight provided through Suspicious Activity Reports (SARs) and other valuable information conveyed by the financial sector have been instrumental in identifying money laundering and other financial schemes associated with the Iranian regime,” added FinCEN Director Kenneth A. Blanco. “This advisory focuses financial institutions’ attention on the current risks associated with transactions involving the Iranian regime. It also provides concrete red flags and typologies to help them identify potentially illicit Iran-linked activity. In so doing, this advisory not only increases industry awareness; it also enhances the future value of related SAR reporting and ultimately strengthens the safety and security of the U.S. financial system.”

The advisory details how the Iranian regime has abused the international financial system through illicit means. For example, the Iranian regime has masked illicit transactions using senior officials of the CBI, who used their official capacity to procure hard currency and conduct transactions for the benefit of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and its terrorist proxy group, Lebanese Hizballah. Accordingly, financial institutions are advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to the Iranian regime and/or designated Iranian persons, and the advisory details examples of exchange house-related schemes. Iran-related actors use front and shell companies around the world in procurement networks through which the Iranian regime has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry.

The advisory further warns financial institutions to be on the lookout for possible evasive practices involving Iranian shipping companies. Financial institutions should also be aware of possible Iranian abuses of virtual currency and precious metals to evade sanctions and gain access to the international financial system and to conceal their nefarious actions.

In order to help financial institutions identify deceptive activity potentially linked to the Iranian regime, FinCEN has included red flags in its advisory. For example, CBI officials’ routing transactions to personal accounts rather than central bank or government-owned accounts, and individuals or entities with no central bank or government affiliation withdrawing funds from such accounts, may be a red flag for financial institutions to investigate. Similarly, wire transfers or deposits that do not contain any information on the source of funds, contain incomplete information about the source of funds, do not match the customer’s line of business, or that involve jurisdictions where there is a higher risk of dealing with entities linked to the Iranian regime may be red flag indicators of illicit Iranian attempts to gain access to the U.S. financial system or evade sanctions.

Following the full re-imposition on November 5, 2018 of sanctions lifted under the Joint Comprehensive Plan of Action (JCPOA), FinCEN expects that Iranian financial institutions, the

Iranian regime, and its officials will increase their efforts to evade U.S. sanctions to fund malign activities and secure hard currency for the Government of Iran. Treasury and the U.S.

Government are interested in information related to the Iranian regime's efforts outlined in this advisory, as well as information pertaining to how the Iranian regime or Iranian entities subject to sanctions, including the CBI, otherwise evade the sanctions and access the U.S. financial system.

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. FinCEN requests that financial institutions reference this advisory by including the key term "Iran FIN-2018-A006" in the SAR narrative and in appropriate SAR fields to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in the advisory.



# FinCEN ADVISORY

FIN-2018-A006

October 11, 2018

## Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help U.S. financial institutions (particularly banks; money services businesses (MSBs), such as virtual currency administrators and exchangers; and dealers in precious metals, stones, and jewels) better detect

### This advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments

potentially illicit transactions related to the Islamic Republic of Iran (Iran). This advisory will also help foreign financial institutions better understand the obligations of their U.S. correspondents, avoid exposure to U.S. sanctions, and address the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) risks that Iranian activity poses to the international financial system.<sup>1</sup>

The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups, ballistic missile development, human rights abuses, support to the Syrian regime, and other destabilizing actions targeted by U.S. sanctions.

This advisory highlights the Iranian regime's exploitation of financial institutions worldwide, and describes a number of typologies used by the regime to illicitly access the international financial system and obscure and further its malign activity. It also provides red flags that may assist financial institutions in identifying these methods.<sup>2</sup> Additionally, this advisory is intended to assist financial institutions in light of the United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the re-imposition of U.S. sanctions previously lifted under the JCPOA following the 90- and 180-day wind-down periods for certain activities, while also reminding financial institutions of regulatory obligations under the Bank Secrecy Act (BSA) and the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA).<sup>3</sup>

1. For general information on U.S. sanctions on Iran, see the "U.S. Sanctions" section on p.15 of this advisory.
2. While this advisory addresses U.S. sanctions that prohibit U.S. persons and U.S.-owned or -controlled foreign entities from engaging in transactions involving Iran, including persons "ordinarily resident" in Iran, financial institutions should not take this to mean that all transactions involving Iran, Iranian citizens, or persons with connections to Iran are suspicious or prohibited. Institutions should instead regard an Iranian nexus and the typologies listed in this advisory as factors to consider when assessing whether any specific transaction or activity has an illicit nexus or is otherwise prohibited.
3. For more information about the withdrawal of the United States from the JCPOA, please see <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180508.aspx> and <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx>.

## Iran's Abuse of the International Financial System

Some of the methods used by the Iranian regime to access the financial system through covert means and to further its malign activities include misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran (CBI). Iran also has a history of using precious metals to evade sanctions and gain access to the financial system and may seek to use virtual currencies in the future. Often, these efforts serve to fund the regime's nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other terrorist groups.

### The Iranian Regime's Use of CBI Officials and Exchange Houses to Facilitate Malign Activity

#### Use of CBI Officials

Senior officials of the CBI have played a critical role in enabling illicit networks, using their official capacity to procure hard currency and conduct transactions for the benefit of the IRGC-QF and its terrorist proxy group, Lebanese Hizballah.<sup>4</sup> The CBI has also been complicit in these activities.

On May 15, 2018, the Office of Foreign Assets Control (OFAC) designated then-CBI Governor Valiollah Seif and the assistant director of the CBI's International Department, Ali Tarzali, adding them to OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) for conducting transactions through Iraq's banking sector for the benefit of the IRGC-QF and Lebanese Hizballah, which has acted as a proxy for the IRGC-QF.<sup>5</sup> Specifically, Valiollah Seif conspired with the IRGC-QF to move millions of dollars, in a variety of currencies, through the international financial system to allow the IRGC-QF to fund its activities abroad. Seif also supported the transfer of IRGC-QF-associated funds to al-Bilad Islamic Bank, an Iraq-based bank that was also designated by OFAC. Ali Tarzali worked with Lebanese Hizballah and proposed that the terrorist group send funds through al-Bilad Islamic Bank. On May 15, 2018, OFAC also designated the Chairman and Chief Executive of al-Bilad Islamic Bank, who acted as an intermediary to enable and conceal these transactions.<sup>6</sup>

Financial institutions should be aware that the U.S. Department of the Treasury has repeatedly observed CBI officials and the IRGC-QF using regional financial institutions as intermediaries to conceal illicit transactions. In exercising appropriate due diligence, financial institutions should be

4. See <https://home.treasury.gov/index.php/news/press-releases/sm0385>. In addition, on [May 15, 2018](#) and [May 17, 2018](#), OFAC issued new designations relating to the Central Bank of Iran and its senior officials.

5. See <https://home.treasury.gov/news/press-releases/sm0385>.

6. See <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180515.aspx> and <https://home.treasury.gov/index.php/news/press-releases/sm0385>.

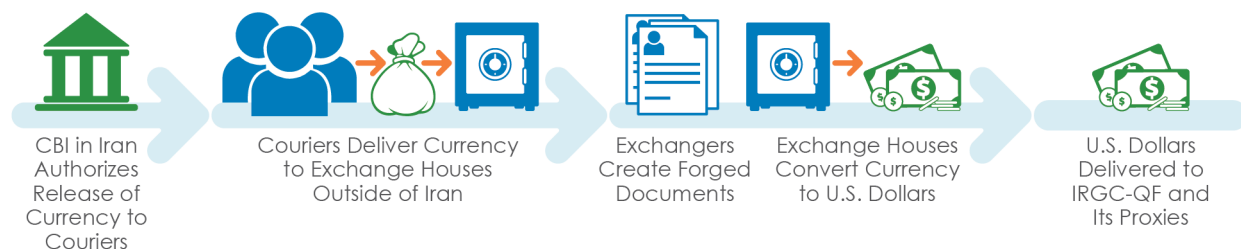
aware that some counterparty financial institutions may not be equipped to identify or address CBI officials’ deceptive transactions.<sup>7</sup> IRGC-QF front companies are known to retrieve funds—some of which are generated by the sale of Iranian oil—in various currencies from foreign bank accounts held by the CBI and then transfer the funds back to Iran.

### Use of Exchange Houses

Financial institutions are also advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to Iran or Iranian persons, given that the Iranian regime, senior CBI officials, and the CBI have used such entities to conceal the origin of funds and procure foreign currency for the IRGC-QF.

For example, on May 10, 2018, the United States, in a joint action with the United Arab Emirates (UAE), disrupted an extensive currency exchange network in Iran and the UAE. The network procured and then transferred millions of U.S. dollar-denominated bulk cash through the UAE to the IRGC-QF. As part of this joint action, OFAC designated six individuals and three entities, including Jahan Aras Kish, the Joint Partnership of Mohammadreza Khedmati and Associates, and the Rashed Exchange.<sup>8</sup> The CBI was complicit in the IRGC-QF’s scheme, actively supported this network’s currency conversion, and enabled it to access funds that it held in its foreign bank accounts. To mask ties to Iran and particularly to the IRGC-QF, this network of cash couriers and currency exchangers established the three now-designated front companies. At least one of these companies, the Rashed Exchange, advertised its currency exchange and international money transfer business all over the world on its website and through social media in an effort to portray its activities as legitimate, while in reality its management was using the company to facilitate the transfers for the IRGC-QF. Khedmati, the managing director of Rashed Exchange, also worked with the IRGC-QF to forge documents to conceal their illicit financial activities from UAE authorities. Using these front companies, these individuals and entities procured and transferred millions in U.S. dollar-denominated bulk cash to the IRGC-QF to fund its malign activities and regional proxy groups.<sup>9</sup>

The diagram below depicts this type of exchange house-related scheme:



7. See <https://home.treasury.gov/news/press-releases/sm0383>.

8. *Ibid.*

9. See <https://home.treasury.gov/index.php/news/press-releases/sm0385>.

As financial institutions are aware, during previous periods of heightened sanctions pressure, Iran relied heavily on third-country exchange houses and trading companies to move funds to evade sanctions.<sup>10</sup> As the sanctions on Iran that were lifted under the JCPOA are coming back into effect, Iranian financial institutions can be expected to increase the use of these or other evasive practices. These practices include the use of third-country exchange houses or trading companies to act as money transmitters in processing funds transfers through the United States to third-country beneficiaries, in support of business with Iran that is not exempt or otherwise authorized by OFAC. These third-country exchange houses or trading companies frequently lack their own U.S. dollar accounts and instead rely on the correspondent accounts of their regional banks to access the U.S. financial system. Often these entities are located in jurisdictions considered high risk for transactions implicating OFAC sanctions, and they appear to process primarily commercial transactions rather than personal remittances, which are authorized by OFAC.

OFAC's January 10, 2013 advisory identified the following evasive practices used by such third-country exchange houses or trading companies: omission of references to Iranian addresses, omission of names of Iranian persons or entities in the originator or beneficiary fields, and transmission of funds without referencing the involvement of Iran or the designated persons.<sup>11</sup>

Financial institutions should be aware when monitoring payments involving third-country exchange houses or trading companies that, as informed by such firms' risk profile, a financial institution may be processing commercial transactions related to Iran or Iranian persons. As appropriate, financial institutions should consider (1) requesting additional information from correspondents on the nature of such transactions and the parties involved; (2) while monitoring these payments, conducting account and transaction reviews for individual exchange houses or trading companies that have repeatedly violated or attempted to violate U.S. sanctions against Iran; and (3) contacting their correspondents that maintain accounts for, or facilitate transactions on behalf of, third-country exchange houses or trading companies that engage in one of the above-referenced examples in order to request additional information and to alert them to the use of these practices.

---

10. Third-country exchange houses are financial institutions licensed to deal in foreign exchange and transmit funds on behalf of individuals and companies. Trading companies are entities that are not licensed to transmit funds, but in practice operate as exchange houses and rely upon their bank accounts to transmit funds on behalf of third parties. See [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110\\_iran\\_advisory\\_exchange\\_house.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf).

11. In 2013, OFAC issued an advisory that highlighted some of the practices used at that time to circumvent U.S. and international economic sanctions concerning Iran, including relying heavily on third-country exchange houses and trading companies to move funds. See [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110\\_iran\\_advisory\\_exchange\\_house.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf). Neither the 2013 OFAC advisory nor this advisory are intended to suggest that U.S. financial institutions close accounts they hold for third-country exchange houses and/or trading companies. Additionally, neither advisory should be interpreted as a signal that third-country exchange houses and/or trading companies are necessarily facilitating illicit finance.



## Iran's Use of Procurement Networks

Malign Iran-related actors use front and shell companies<sup>12</sup> around the world to procure technology and services that allow them to evade sanctions and continue their destabilizing behaviors.

Through these procurement networks, Iran has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry. As part of a risk-based approach, financial institutions should familiarize themselves with these deceptive practices and take steps to avoid direct or indirect facilitation of them.

### Printing Equipment and Materials for Counterfeiting Currency

In November 2017, OFAC designated two individuals, Reza Heidari and Mahmoud Seif, and four entities, Pardazesh Tasvir Rayan Co., ForEnt Technik GmbH Co., Printing Trade Center GmbH, and Tejarat Almas Mobin Holding, for their respective roles assisting the IRGC-QF to counterfeit currency. This network used two German-based front companies to deceive European suppliers, circumvent European export restrictions, and surreptitiously procure advanced printing machinery, security printing machinery, and raw materials such as watermarked paper and specialty inks. The network used these items to print counterfeit Yemeni bank notes for the IRGC-QF. Mahmoud Seif was previously involved with the procurement of weapons for the IRGC-QF.<sup>13</sup>

### Dual-Use Equipment Procurement for Ballistic Missile Proliferation

In February 2017, OFAC designated multiple individuals and entities that are part of the Abdollah Asgharzadeh network for the procurement of dual-use and other goods on behalf of organizations involved in Iran's ballistic missile programs. This network coordinated procurement through intermediary companies that obfuscated the final recipient of the goods. Asgharzadeh and his associates relied on a network of trusted China-based brokers and their companies to assist his procurement of dual-use and other goods.<sup>14</sup>

---

12. Shell companies are typically non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. See FinCEN Guidance [FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies"](#) (November 2006) and SAR Activity Review: [Issue 1](#) (October 2000), [Issue 2](#) (June 2001), and [Issue 7](#) (August 2004).

13. See <https://www.treasury.gov/press-center/press-releases/Pages/sm0219.aspx>.

14. OFAC also designated MKS International, a UAE-based company that used multiple front companies in order to circumvent export laws and sanctions to procure technology and/or materials to support Iran's ballistic missile program, as well as for acting for or on behalf of, or providing support to, Iran's IRGC-QF. See <https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx>.

## Commercial Aviation Industry

Designated Iranian airlines and their agents and affiliates have used deceptive schemes to procure aviation-related materials using front companies. Treasury has issued numerous rounds of sanctions related to efforts by designated Iranian airlines to evade sanctions via the use of front or shell companies.<sup>15</sup>

Financial institutions providing services to the commercial aviation industry should be aware of prior actions by designated Iranian airlines to evade sanctions, and they are advised to exercise appropriate due diligence to ensure compliance with legal requirements. Foreign financial institutions are reminded that they may be subject to sanctions for knowingly conducting significant transactions for or with certain Iran-related persons<sup>16</sup> (such as Mahan Air, Caspian Air, Dena Airways, Meraj Air, Pouya Air, Al-Naser Wings Airlines, Syrian Air, Khors Aircompany, Dart Airlines, and UM Air), including prohibitions or strict conditions on their ability to open or maintain correspondent or payable-through accounts in the United States. Non-U.S. persons, including foreign financial institutions, may also be subject to designation and listing on the SDN List for, e.g., providing material support to designated Iranian airlines.

### **Mahan Air**

For many years, the Iranian commercial airline Mahan Air has transferred weapons, funds, and people on behalf of the IRGC-QF and provided support to the Syrian Assad regime and Lebanese Hizballah. In 2011, OFAC designated Mahan Air for providing financial, material, and technological support to the IRGC-QF. To evade sanctions, Mahan Air front companies have negotiated sales contracts and obtained U.S. parts and services for Mahan Air's aircraft in violation of U.S. sanctions.<sup>17</sup> These front companies facilitate the transfer of funds to vendors and service providers on behalf of Mahan Air, while also aiding in the procurement of goods, such as aviation parts and services from neighboring countries, Europe, and Asia. The aviation-related materials are then shipped to either the same company, or a different front company,

15. For example, front companies or other companies that have been designated by OFAC for assisting designated Iranian airline Mahan Air in procuring aircraft and related parts and services include Blue Sky Aviation Co FZE; Pioneer Logistics; Asian Aviation Logistics; Avia Trust FZE; Grandeur General Trading FZE ; Aviation Capital Solutions; Aircraft, Avionics, Parts & Support Ltd.; and HSI Trading FZE. For OFAC press releases related to Mahan Air sanctions see [October 12, 2011](#); [September 19, 2012](#); [May 31, 2013](#); [February 6, 2014](#); [August 29, 2014](#); [May 21, 2015](#); [March 24, 2016](#); [September 14, 2017](#); [October 16, 2017](#); [May 24, 2018](#); and [July 9, 2018](#) at <https://home.treasury.gov/news/press-releases>.

16. These Iran-related persons include: (1) Iranian persons on the SDN List; (2) the IRGC and its designated agents or affiliates; and (3) any other person on the SDN List designated in connection with Iran's proliferation of weapons of mass destruction or their means of delivery or Iran's support for international terrorism.

17. See <https://www.treasury.gov/press-center/press-releases/Pages/jl2618.aspx>, <https://www.treasury.gov/press-center/press-releases/Pages/jl0395.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx>.



sometimes in another country, to be forwarded to Iran. Mahan Air has moved payments through several front companies and financial institutions in the United States, Canada, the United Kingdom, Belize, France, Belgium, Czech Republic, the UAE, Bahrain, Saudi Arabia, Kyrgyzstan, Sri Lanka, and Bangladesh.

Mahan Air and other designated Iranian airlines' use of front companies is illustrated by recent Treasury actions targeting a procurement network. For example, on May 24, 2018, Treasury designated a network of Turkish front companies that procured U.S.-origin parts for Mahan Air. This network purchased aviation parts—including export-controlled U.S. goods such as U.S.-origin engines—from foreign vendors. The parts were delivered to Istanbul and then forwarded to Mahan Air.<sup>18</sup> OFAC has previously designated airlines in Ukraine, Kyrgyzstan, and Iraq that have served as intermediaries for Mahan Air to acquire aircraft, as well as front companies in the UAE, Thailand, Turkey, and the United Kingdom that purchase parts or facilitate payments on behalf of Mahan Air. For example, in May 2015, Treasury designated Iraq-based Al-Naser Airlines, now operating as Al-Naser Wings Airlines, for purchasing nine Airbus aircraft for Mahan Air from unwitting European suppliers. Al-Naser Airlines also attempted to purchase at least two Airbus aircraft located in the United States for Mahan Air, with payments for the planes wired from the account of a Dubai-based general trading company. Additionally, on July 9, 2018, Treasury designated a Malaysia-based general sales agent (GSA) of Mahan Air, Mahan Travel and Tourism Sdn Bhd, which provides Mahan with reservation and ticketing services. This action notified to the aviation community of the sanctions risk of maintaining commercial relationships with Mahan Air.<sup>19</sup> Likewise, on September 14, 2018, Treasury designated Thailand-based My Aviation Company Limited for acting for or on behalf of Mahan Air. This Thailand-based company disregarded numerous U.S. warnings, issued publicly and delivered bilaterally to the Thai government, to sever ties with Mahan Air.<sup>20</sup>

---

18. See <https://home.treasury.gov/news/press-releases/sm0395>.

19. See <https://home.treasury.gov/news/press-releases/sm423>.

20. See <https://home.treasury.gov/news/press-releases/sm484>.

## Iran-Related Shipping Companies' Access to the Financial System

During previous periods of heightened sanctions pressure, Treasury identified Iranian or Iran-related companies using deceptive shipping practices to evade U.S. sanctions. As detailed in previous OFAC advisories and designation actions, these practices include: the use of falsified documents,<sup>21</sup> the reflagging of vessels,<sup>22</sup> and the involvement of third parties, such as brokers and trading companies, to mask the underlying payments and business activity with Iran.<sup>23</sup> For example, in the pre-JCPOA period, Treasury identified shipping companies around the world that falsified documents to hide ships docking in Iranian ports and the accompanying trade-related payments. In addition, in the past, as the United States has added entities or individuals to OFAC's SDN List, there have been instances where a vessel's ownership or operation was transferred from a newly-designated person to a front company or other person acting for or on behalf of the designated person.<sup>24</sup>

As the sanctions on Iran that were lifted under the JCPOA come back into effect following the 90- and 180-day wind-down periods, Iranian shipping companies may return to the use of these or other evasive practices. Financial institutions may see indications of these deceptive shipping practices in the information contained in international wires, payment requests, and letters of credit. Documents may also be falsified, and include bills of lading and shipping invoices to conceal shipping routes, embarkation ports, or shipping agents. Financial institutions may find maritime databases and reports—such as those generated by the International Maritime Bureau or other available services—helpful when verifying trade-related documents.<sup>25</sup> Financial institutions should be aware of changes regarding the issuing or writing of letters of credit and other trade-related financial transactions. Financial institutions should report those changes in their SAR filings if the changes appear to be related to malign activity. In addition, among other deceptive conduct, Iranian vessels may attempt to hide their origin and purpose by potentially fabricating

- 
21. See [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20110331\\_advisory.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20110331_advisory.pdf). In this March 31, 2011 advisory, OFAC alerted shippers, importers/exporters, and freight forwarders to practices used by the Islamic Republic of Iran Shipping Lines (IRISL), which at the time was designated pursuant to E.O. 13382, and companies acting on its behalf to evade U.S. and international economic sanctions by hiding the involvement of IRISL in shipping transactions, including (1) using container prefixes registered to another carrier; (2) omitting or listing invalid, incomplete, or false container prefixes in shipping container numbers; and/or (3) naming non-existent ocean vessels in shipping documents. See <https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx>. IRISL and its affiliates, as well as a large number of vessels in which these entities held an interest, were removed from OFAC's SDN List on January 16, 2016 in connection with the JCPOA. No later than November 5, 2018, OFAC will re-impose, as appropriate, the sanctions that applied to persons removed from SDN List and/or other lists maintained by OFAC on January 16, 2016.
  22. See [https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ofac\\_irisl\\_advisory\\_07192012.pdf](https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ofac_irisl_advisory_07192012.pdf). In this July 19, 2012 advisory, OFAC alerted the maritime industry that IRISL operated vessels despite their flags having been revoked. International sanctions at the time, and IRISL's efforts to evade them through deceptive practices, led to increased vigilance by the maritime industry and prompted an increasing number of countries to revoke or refuse to issue a flag to vessels in which IRISL or its affiliates had an interest. See <https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/jl1933.aspx>.
  23. See <https://www.treasury.gov/press-center/press-releases/Pages/TG981.aspx>.
  24. See <https://www.treasury.gov/press-center/press-releases/Pages/jl1933.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/TG981.aspx>.
  25. See <https://www.icc-ccs.org/icc/imb>.

vessel registration and flag credentials at ports of call and canal entrances. Malign Iran-related actors and sanctioned entities engage in these activities to bypass financial institutions' SDN filters so they may evade sanctions. Financial institutions should continue to conduct appropriate due diligence to ensure they are not directly or indirectly providing services to sanctioned parties.

## **The Iranian Regime's Illicit Use of Precious Metals**

Iran has previously used precious metals, such as gold, to evade U.S. sanctions and facilitate the sale of Iranian oil and other goods abroad. In response to these schemes, the United States enacted sanctions specifically targeting Iran's trade in precious metals, including section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012. As the United States re-imposes sanctions lifted under the JCPOA, financial institutions should be aware of prior schemes used by entities with a nexus to Iran to evade sanctions using gold and other commodities.

## **Virtual Currency**

Since 2013, Iran's use of virtual currency includes at least \$3.8 million worth of bitcoin-denominated transactions per year. While the use of virtual currency in Iran is comparatively small, virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions. Despite public reports that the CBI has banned domestic financial institutions from handling decentralized virtual currencies, individuals and businesses in Iran can still access virtual currency platforms through the Internet. For example, virtual currency can be accessed through: (1) Iran-located, Internet-based virtual currency exchanges; (2) U.S.- or other third country-based virtual currency exchanges; and (3) peer-to-peer (P2P) exchangers.

Institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran. Institutions should also be aware that the international virtual currency industry is highly dynamic; new virtual currency businesses may incorporate or operate in Iran with little notice or footprint. Further, P2P exchangers—natural or legal persons who offer to buy, sell, or exchange virtual currency through online sites and in-person meetups—may offer services in Iran. These P2P exchangers may operate as unregistered foreign MSBs in jurisdictions that prohibit such businesses; where virtual currency is hard to access, such as Iran; or for the purpose of evading the prohibitions or restrictions in place against such businesses or virtual currency exchanges and other similar business in some jurisdictions. Institutions can utilize technology created to monitor open blockchains and investigate transactions to or from P2P exchange platforms.

Activity of these exchangers may involve wire transactions from many disparate accounts or locations combined with transfers to or from virtual currency exchanges. These transactions may occur when account holders fund an account or withdraw value from an account, especially if the foreign exchanger operates in multiple currencies.

Financial institutions and virtual currency providers that have BSA and U.S. sanctions obligations should be aware of and have the appropriate systems to comply with all relevant sanctions requirements and AML/CFT obligations. Sanctions requirements may include not only screening

against the SDN List but also appropriate steps to comply with other OFAC-administered sanctions programs, including those that impose import and/or export restrictions with respect to particular jurisdictions.<sup>26</sup> Further, a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/CFT obligations and OFAC jurisdiction.

U.S. individuals and institutions involved in virtual currency should be aware of OFAC's March 2018 Frequently Asked Questions (FAQs) on sanctions issues associated with virtual currencies.<sup>27</sup> The FAQs remind U.S. persons that their compliance obligations with respect to transactions are the same, regardless of whether a transaction is denominated in virtual currency or not. OFAC also states as a general matter that U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms subject to OFAC jurisdiction that facilitate or engage in online commerce or process transactions using "digital currency," are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions.<sup>28</sup> Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities. Additionally, persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority.<sup>29</sup>

## **Financial Action Task Force's Findings Related to Iran's Anti-Money Laundering/Combating the Financing of Terrorism Regime**

The Financial Action Task Force (FATF) has listed Iran as a jurisdiction with systemic deficiencies in its AML/CFT regime. Despite Iran's commitment in June 2016 to an action plan with the FATF to address its AML/CFT deficiencies, Iran has failed to complete the majority of its action plan. The FATF therefore continues to call upon its members and all jurisdictions to advise their financial institutions to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from Iran.

In addition to keeping Iran on its Public Statement, on June 29, 2018, the FATF expressed disappointment with Iran's failure to implement its action plan, and it reiterated its concern with the terrorist financing risk emanating from Iran and the threat this poses to the international financial system. The FATF noted that Iran "should fully address its remaining action items, including by: (1) adequately criminalising terrorist financing, including by removing the exemption for designated groups 'attempting to end foreign occupation, colonialism and racism'; (2) identifying and freezing terrorist assets in line with the relevant United Nations Security Council

---

26. If a financial institution or virtual currency provider has questions concerning OFAC sanctions, they can either call OFAC's Toll-Free Hotline at 1-800-540-6322, or email OFAC's Feedback Account at [OFAC\\_Feedback@treasury.gov](mailto:OFAC_Feedback@treasury.gov).

27. See FAQ 559 to 563, available at [https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\\_compliance.aspx](https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx).

28. For the purposes of OFAC sanctions programs, the term "digital currency" includes digital fiat currency or sovereign cryptocurrency, virtual currency (non-fiat), and digital representations of fiat currency.



29. See FAQ 560, available at [https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq\\_compliance.aspx](https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx).

resolutions; (3) ensuring an adequate and enforceable customer due diligence regime; (4) ensuring the full independence of the Financial Intelligence Unit and requiring the submission of STRs [Suspicious Transaction Reports] for attempted transactions; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF [Terrorist Financing] Conventions and clarifying the capability to provide mutual legal assistance; (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information; (8) establishing a broader range of penalties for violations of the ML [Money Laundering] offense; and (9) ensuring adequate legislation and procedures to provide for confiscation of property of corresponding.”<sup>30</sup> The FATF will decide upon the appropriate action in October 2018 if Iran has not by then enacted the necessary amendments to its AML and CFT laws and ratified the Terrorist Financing and Palermo Conventions. All available advisories on FATF Plenaries, including previous years, are available at <https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories>.

## Red Flags Related to Deceptive Iranian Activity

The following red flags may help financial institutions identify suspicious activity involving the schemes discussed above. In applying these red flags, financial institutions are advised that no single transactional red flag necessarily indicates suspicious activity, and institutions should ensure that their assessments are in line with their internal risk profile. Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer’s historical financial activity and the existence of other red flags, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate. Foreign financial institutions may find the information beneficial for their risk and threat assessments and suspicious transaction reporting requirements. The appropriate financial crimes compliance/sanctions compliance within the financial institution should be apprised of any transactions that are determined to involve Iran.

### Illicit Activity by the CBI or Its Officials

-  **1 Use of Personal Account.** The CBI or CBI officials route transactions to personal accounts instead of central bank or government-owned accounts. Individuals or entities with no central bank or government affiliation withdraw funds from such accounts.
-  **2 Unusual Wire Transfers.** The CBI engages in multiple wire transfers to banks or financial institutions that the CBI would not normally engage in, or that are not related to traditional central bank activity.<sup>31</sup>

30. See <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2018.html>.

31. Effective November 5, 2018, foreign financial institutions will be subject to correspondent or payable-through account sanctions for conducting or facilitating certain significant financial transactions with the CBI, pursuant to section 1245 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA).



**3** *Use of Forged Documents.* Front companies acting for or on behalf of designated persons use forged documents to conceal the identity of parties involved in the transactions. For example, as a part of the IRGC-QF’s currency exchange network scheme, documents were forged by an IRGC-QF front company manager to mislead authorities and conceal the true customers of the entities involved in the scheme.

### Illicit Activity through Exchange Houses

**4** *Use of Multiple Exchange Houses.* Customers may have transactions moving through multiple exchange houses, adding additional fees and costs as they progress through the system. The fees, number of transactions, and patterns of transactions are atypical to standard and customary commercial practices.

**5** *Multiple Depositors.* Account holders that receive deposits—that do not appear to match the customer’s profile or provided documentation—from numerous individuals and entities.

### Use of Procurement Networks

**6** *Shell or Front Companies.* Transactions involving companies that originate with, or are directed to, entities that are shell corporations, general “trading companies”, or companies that have a nexus with Iran. For example, a company has an affiliate in Iran or is owned by individuals known to be loyal to the Iranian regime, and appears to lack a general business purpose. Iran uses front companies incorporated across the world, including in Asia and Europe. Other indicators of possible shell companies include opaque ownership structures, individuals/entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies.

**7** *Suspicious Declarations.* Declarations of information that are inconsistent with other information, such as previous transaction history or nature of business. Declarations of goods that are inconsistent with the associated transactional information.

**8** *Unrelated Business.* Transactions that are directed to companies that operate in unrelated businesses, and which do not seem to comport with the Customer Due Diligence (CDD) and other customer identification information collected during client onboarding and subsequent refreshes.

### Illicit Procurement of Aircraft Parts

**9** *Use of Front Companies and Transshipment Hubs to Source Aircraft Parts.* Financial institutions that facilitate commercial aviation-related financial transactions where the beneficial ownership of the counterparty is unknown and the delivery destination is a common transshipment point for onward delivery to Iran. Iran-linked persons have attempted to source U.S.-origin aircraft and related parts from third countries known to be hubs for maintenance, repair, and overhaul operations, and then use front companies located in third-countries to conceal or obfuscate the ultimate Iranian beneficiary of the U.S.-origin aircraft, parts, and aviation-related materials.

**10** *Misrepresentation of Sanctions.* Misrepresenting to suppliers, dealers, brokers, re-insurers, and other intermediaries that sanctions against Iran have been lifted or are no longer applicable as a result of the JCPOA, or falsely claiming without supporting documentation that an OFAC license has been obtained.

### Iran-Related Shipping Companies' Access to the U.S. Financial System

**11** *Incomplete and Falsified Documentation.* Transactions and wire transfers that include bills of lading with no consignees or involving vessels that have been previously linked to suspicious financial activities. Documentation, such as bills of lading and shipping invoices, submitted with wire and payment requests that may appear to be falsified, or with key information omitted, in an attempt to hide the Iranian nexus.

**12** *Inconsistent Documentation for Vessels Using Key Ports.* Inconsistencies between shipping-related documents and maritime database entries that are used for conducting due diligence. For example, the maritime database may indicate that a vessel docked in an Iranian port, even though this information is not included in the shipping documents submitted to financial institutions for payment processing. Major ports in Iran are Bandar Abbas, Assaluyeh, and Bandar-e Imam Khomeyni, which is also known as Abadan. Port cities on the Gulf include: Ahvaz, Bushehr, Bandar-e Lengeh, Bandar-e Mahshahr, Chabahar, Kharg Island, and Lavan Island. Kharg Island and Lavan Island are major oil and gas ports.

**13** *Previous Ship Registration to Sanctioned Entities.* Vessels whose ownership or operation is transferred to another person—following OFAC’s designation of its owner or operator—on behalf of the designated person, but the designated owner or operator maintains an interest in the vessel.

### Suspicious Funds Transfers

**14** *Lack of Information Regarding Origin of Funds.* Wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer’s line of business.

**15** *Unusual or Unexplainable Wire Transfers.* Multiple, unexplained wire transfers and transfers that have no apparent connection to a customer’s profile. For example, individuals may claim that the unusually high-value wire transfers they receive from one or more foreign countries are merely funds sent from relatives in Iran. In addition, wire transfers to accounts in the United States from high-risk jurisdictions that have no apparent connection to the customer’s line of business.

- 16** *Using Funnel Accounts.* Third parties from across the United States who deposit funds into the accounts of U.S.-based individuals with ties to Iran.<sup>32</sup> The deposits and associated transactions do not match the account holder’s normal geographical footprint, and the source of the funds is unknown or unclear.
  
- 17** *Structuring Transactions.* U.S. persons send or receive money to or from Iran by structuring the cash portion of the transactions to avoid the currency transaction reporting threshold of \$10,000. Individuals returning to the United States from Iran also may make large deposits of monetary instruments rather than cash.
  
- 18** *Gold.* Given Iran’s prior use of gold as a substitute for cash to evade U.S. sanctions, financial institutions should consider conducting additional due diligence on transactions related to precious metals, particularly in geographic regions in close proximity to Iran (such as Turkey) that engage in significant gold-related transactions. Additionally, financial institutions may notice transactions not obviously linked to Iran, but related to the purchase of unusually high volumes of gold.

### Virtual Currency

- 19** *Logins from Iranian Internet Protocol Addresses or with Iranian Email.* Internet Protocol (IP) login activity from entities in Iran or using an Iranian email service in order to transact virtual currencies through a virtual currency exchange. In such cases, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps, device identifiers, and indicators of compromise that can provide helpful information to authorities.<sup>33</sup>
  
- 20** *Payments to/from Iranian Virtual Currency Entity.* A customer or correspondent payment to or from virtual currency exchanges that appear to be operating in Iran.
  
- 21** *Peer-to-Peer (P2P) Exchangers.* Unexplained transfers into a customer account from multiple individual customers combined with transfers to or from virtual currency exchanges. Wire transfers are usually associated with funding an account or withdrawing value, especially with foreign exchanges that may operate in multiple currencies.

---

32. Funnel account activity often involves a customer structuring currency deposits into an account in one geographic area, with the funds subsequently withdrawn in a different geographic region with little time elapsing between deposit and withdrawal. The rapid flow of funds may also span a large geographic area between the deposits and withdrawals, including instances where the deposit location is thousands of miles away from the withdrawal location. In some instances, these disparate deposits have been consolidated into a single account and withdrawn from the consolidated account. The currency deposits and withdrawals often have no apparent lawful or business purpose and do not reflect the stated occupation of the account holder. For a detailed description of funnel accounts, see <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a006> and <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005>.

33. See Question #1 in “FAQs regarding the Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs” (October 2016) as well as “Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime,” available at: [https://www.fincen.gov/sites/default/files/shared/FAQ\\_Cyber\\_Threats\\_508\\_FINAL.PDF](https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF) and [https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508\\_2.pdf](https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf).



FinCEN expects that Iranian financial institutions, the Iranian regime, and its officials will increase their efforts to evade U.S. sanctions to fund malign activities and secure hard currency for the Government of Iran, following the re-imposition of sanctions lifted under the JCPOA. Treasury and the U.S. Government are interested in information related to Iran’s efforts outlined in this advisory, as well as information pertaining to how Iran or Iranian entities subject to sanctions, including the CBI, otherwise evade the sanctions and access the U.S. financial system.

This advisory does not describe all of the methods the Government of Iran may use to gain access to the U.S. financial system or evade sanctions, such as using funnel accounts or informal value transfer systems (IVTS).<sup>34</sup> FinCEN encourages financial institutions to review past advisories relating to Iran, including FinCEN Advisory FIN-2018-A004 “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies” (September 2018),<sup>35</sup> FinCEN Advisory FIN-2010-A008 “Update on the Continuing Illicit Finance Threat Emanating from Iran” (June 2010),<sup>36</sup> FinCEN Advisory FIN-2008-A002 “Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity” (March 2008),<sup>37</sup> and FinCEN Advisory FIN-2007-A001 “Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity” (October 2007).<sup>38</sup>

## U.S. Sanctions

U.S. primary sanctions on Iran are those sanctions administered by OFAC that broadly prohibit U.S. persons and U.S.-owned or -controlled foreign entities from engaging in virtually all transactions or dealings with or involving Iran, the Government of Iran, or Iranian financial institutions, unless the transactions are exempt from regulation or expressly authorized by the U.S. Government.<sup>39</sup> These prohibitions also apply to transactions in or transiting through the United States, as well as other types of activities. Section 560.204 of the Iranian Transactions and Sanctions Regulations (ITSR) prohibits the exportation of goods, services (including financial services), or technology directly or indirectly from the United States, or by a U.S. person, to Iran. Pursuant to this provision, U.S. financial institutions are prohibited from opening or maintaining correspondent accounts for or on behalf of Iranian financial institutions. Absent an exemption or OFAC authorization, foreign persons, including foreign financial institutions, are prohibited from processing transactions to or through the United States in violation of this provision, including transactions through U.S. correspondent accounts for or on behalf of Iranian financial institutions, other Iranian persons, or where the benefit is otherwise received in Iran.

34. The term Informal Value Transfer System (IVTS), as originally stated in the March 2003 “IVTS Advisory,” refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. *See* <https://www.fincen.gov/sites/default/files/shared/advis33.pdf>.

35. *See* <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-a004>.

36. *See* <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2010-a008>.

37. *See* <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2008-a002>.

38. *See* <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2007-a001>.

39. *See* Iranian Transactions and Sanctions Regulations, 31 CFR Part 560.

The importation into the United States of any goods or services of Iranian origin or owned or controlled by the Government of Iran is also prohibited unless exempt from regulation or expressly authorized by the U.S. Government. There are also prohibitions on re-exports by non-U.S. persons of goods with 10 percent or more controlled U.S. origin content.

U.S. persons are also subject to broad prohibitions on dealings with, and must block the property and interests in property of, among others, Iran-related persons designated pursuant to authorities targeting specific malign conduct, such as support for terrorism, proliferation of weapons of mass destruction or their means of delivery, and human rights abuses.<sup>40</sup> All Iranian financial institutions are blocked under Executive Order 13599 and section 560.211 of the ITSR and, absent an exemption or OFAC authorization, U.S. persons must block the property and interests in property of all Iranian financial institutions.

Pursuant to the Iranian Financial Sanctions Regulations (IFSR) and multiple statutory and executive authorities, foreign financial institutions may be subject to sanctions for knowingly conducting significant transactions for or with certain Iran-related persons, including prohibitions or strict conditions on their ability to open or maintain correspondent or payable-through accounts in the United States. Non-U.S. persons, including foreign financial institutions, may also be subject to blocking sanctions for, e.g., providing material support to designated persons. U.S. and non-U.S. financial institutions should be conscious of their obligations under OFAC sanctions to prevent any use (both direct and indirect) of their U.S. correspondent accounts for transactions involving an Iranian financial institution. OFAC has issued penalties to both U.S. and non-U.S. financial institutions for processing prohibited transactions through the U.S. financial system that involve an indirect, underlying interest of Iranian individuals and entities, including Iranian financial institutions. As a result, the industry should continue to develop controls designed to curtail indirect involvement of Iranian persons in transactions that transit through or otherwise involve the U.S. financial system. In many cases, this requires institutions to employ higher Know-Your-Customer (KYC) and CDD requirements for Iranian entities or clients who do business with Iran.

In addition, U.S. and non-U.S. financial institutions should continue to implement robust and multi-tiered levels of screening and review for transactions originating from or otherwise involving jurisdictions in close proximity to Iran. Financial institutions engaged in cross-border wire activity should be aware of transactions involving jurisdictions with strong geographical and economic ties to Iran. These practices generally result in significant oversight of correspondent accounts that may involve Iranian interests, as well as create a relatively high-degree of vigilance related to payments and funds transfers on behalf of Iran-related individuals and entities.

Additional information on these sanctions, including sanctions that are being re-imposed following the withdrawal of the United States from the JCPOA, can be found at <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx#legal>.

40. See, e.g., E.O. 13224 and the Global Terrorism Sanctions Regulations, 31 CFR Part 594; E.O. 13382 and the Weapons of Mass Destruction Proliferators Sanctions Regulations; and E.O. 13553 and the Iranian Human Rights Abuses Sanctions Regulations, 31 CFR Part 562.

## Reminder of Regulatory Obligations for U.S. Financial Institutions

Consistent with existing regulatory obligations, U.S. financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with individuals and entities involved in laundering illicit proceeds, including those associated with sanctions evasion.

### **Reminder of AML and Regulatory Obligations for U.S. Financial Institutions Regarding Due Diligence, Correspondent Accounts, CISADA, and Suspicious Activity Reporting**

FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting these risk-based due diligence obligations and to help identify individuals who are providing financial facilitation for or on behalf of sanctioned individuals and entities.

#### *Enhanced Due Diligence Obligations for Private Banking Accounts*

In addition to these general risk-based due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, U.S. financial institutions have regulatory obligations to implement a due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.<sup>41</sup>

#### *Customer Due Diligence and Identification of Beneficial Owners of New Legal Entity Accounts*

As of May 11, 2018, FinCEN's CDD Rule requires banks; brokers or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.<sup>42</sup> This could facilitate the identification of legal entities that may be owned or controlled by individuals and entities impacted by Iran-related sanctions.

41. See 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition of "non-U.S. person" is found in 31 CFR § 1010.605(h).

42. See 31 CFR § 1010.230 (describing beneficial ownership requirements for legal entity customers).

### General Obligations for Correspondent Account Due Diligence and Anti-Money Laundering Programs

U.S. financial institutions also are reminded to comply with their general due diligence obligations under 31 CFR § 1010.610(a), in addition to their general AML Program obligations under 31 U.S.C. § 5318(h) and its implementing regulations.<sup>43</sup> As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for foreign financial institutions, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States.

### Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010

FinCEN also reminds U.S. banks of the reporting requirements associated with *Comprehensive Iran Sanctions, Accountability, and Divestment Act* (CISADA) under 31 CFR § 1060.300, upon receipt of a written request from FinCEN, to inquire of a specified foreign bank for which it maintains a correspondent account, for information with respect to the following: whether the foreign bank maintains a correspondent account for, or has processed transfers of funds on behalf of, an Iranian-linked financial institution designated under the International Emergency Economic Powers Act (IEEPA); and whether the foreign bank has processed transfers of funds for the IRGC or any of its agents or affiliates designated under IEEPA.<sup>44</sup>

### Suspicious Activity Reporting

A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, which may include sanctions evasion.<sup>45</sup>

43. See 31 CFR § 1010.210 (regarding anti-money laundering program requirements).

44. See 31 CFR § 1060.300(a).

45. See generally 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320

### SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. **FinCEN further requests that financial institutions reference this advisory by including the key term:**

**“Iran FIN-2018-A006”**

to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

### For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at [FRC@fincen.gov](mailto:FRC@fincen.gov).

**Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

Financial institutions or virtual currency providers having questions concerning OFAC sanctions should either call OFAC’s Toll-Free Hotline at 1-800-540-6322, or email OFAC’s Feedback Account at [OFAC\\_Feedback@treasury.gov](mailto:OFAC_Feedback@treasury.gov).

**The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.**