FinReg
Davis Polk Insights on Financial Regulation

# As Sanctions "Snap-Back" Approaches, FinCEN Advisory Emphasizes Risks to the U.S. and International Financial Systems Posed by Iran

By John B. Reynolds, Jeanine P. McGuinness, Will Schisa & Britt Mosman on October 15, 2018

POSTED IN ANTI-MONEY LAUNDERING, ECONOMIC SANCTIONS, GUIDANCE & FAQS

On October 11, 2018, the Treasury Department's Financial Crimes Enforcement Network ("**FinCEN**") issued a lengthy "**Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System**," (the "**Iran Advisory**"), which provides examples and typologies of the Iranian regime's exploitation of financial institutions worldwide, and identifies a number of "red flags" intended to assist financial institutions in identifying malign Iranian activity. According to FinCEN, the Iran 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, while also reminding financial institutions of regulatory obligations under the Bank Secrecy Act and the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010. As the November 5, 2018 date for full re-imposition of secondary sanctions waived under the JCPOA grows near, the publication of the Iran Advisory is a further signal that the U.S. Government is moving **aggressively** to isolate Iran financially and economically.

In stark terms, the Iran Advisory warns both U.S. and non-U.S. financial institutions to be conscious of their obligations under sanctions administered by the Treasury Department's Office of Foreign Assets Control ("**OFAC**") to prevent any use (both direct and indirect) of their U.S. correspondent accounts for transactions involving an Iranian financial institution, and to 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 and Customer Due Diligence ("**CDD**") requirements for Iranian entities or clients who do business with Iran.

In addition, FinCEN advises U.S. and non-U.S. financial institutions to 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.

The advisory largely details past Iranian efforts to evade sanctions or engage in illicit financial activity from prior announcements of sanctions designations and other public releases by OFAC. The typologies discussed include misusing banks and **exchange houses**, operating **procurement networks** that utilize **front** or **shell** companies, **exploiting commercial shipping,** masking illicit transactions using **senior officials**, including those at the Central Bank of Iran ("**CBI**"), and using precious metals to evade sanctions and gain access to the financial system. FinCEN also warns that Iran may seek to use virtual currencies in the future to attempt to evade sanctions, and notes that it 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.

In addition, the Iran Advisory notes that the Financial Action Task Force ("**FATF**") has listed Iran as a jurisdiction with systemic deficiencies in its anti-money laundering ("**AML**")/countering the financing of terrorism ("**CFT**") regime and that Iran has failed to implement most of its action plan with the FATF to address its AML/CFT deficiencies. FATF is expected to decide **this month** upon appropriate action if Iran has not enacted necessary amendments to its AML and CFT laws and ratified the Terrorist Financing Convention (the UN International Convention for the Suppression of the Financing of Terrorism) and the Palermo Convention (the UN Convention Against Transnational Organized Crime).

The specific “red flags” identified in the Iran Advisory include the following:

Illicit Activity by the CBI or CBI Officials

- *Use of Personal Accounts*. 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
- *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.
- *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.

Illicit Activity Through Exchange Houses

- *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.
- *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

- *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. 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.

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

Illicit Procurement of Aircraft Parts

- *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.
- *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

- *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.
- *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 Emam Khomenyi, 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.

- *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

- *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.
- *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.
- *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. 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.
- *Structuring Transactions*. 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.
- *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

*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. The Iran Advisory also specifically notes that financial institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran.

- *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.
- *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

FinCEN notes that Treasury and the U.S. Government are interested in information related to Iran's efforts outlined in the Iran 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. Financial institutions filing Suspicious Activity Reports concerning activity of the type described in the Iran Advisory are requested to include the reference term "Iran FIN-2018-A006," to alert FinCEN to this connection.