International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

FinCEN Releases Advisory for Banks, MSBs on Potentially Illicit Transactions with Iran

October 22, 2018

Contact

Jonathan Poling
Partner
jpoling@akingump.com
Washington, D.C.
+1 202.887.4029

Nnedinma Ifudu Nweke
Senior Counsel
nifudu@akingump.com
Washington, D.C.
+1 202.887.4013

Jung Hwa Song
Associate
jsong@akingump.com
New York
+1 212.872.8020

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

Michael Adame
Law Clerk (not admitted to practice)
madame@akingump.com
Washington, D.C.
+1 202.887.4323

Key Points

- On October 11, 2018, FinCEN released an advisory to help U.S. financial institutions better detect potentially illicit transactions related to Iran.
- The advisory describes how Iran attempts to access the international financial system and avoid U.S. sanctions and other financial controls, and it identifies certain red flags indicative of a transaction's potential ties to Iran.
- Financial institutions should expect regulators' increased scrutiny of certain transactions, and compliance obligations generally, with the United States' withdrawal from the JCPOA.

Background

On October 11, 2018, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) released an advisory to help U.S. financial institutions better detect potentially illicit transactions related to the Islamic Republic of Iran ("Iran"). In particular, the advisory targets banks; money services businesses (MSBs), such as virtual currency administrators and exchanges; and dealers in precious metals, stones and jewels.

Iran's Attempts to Access the International Financial System

FinCEN's advisory summarizes the ways the Iranian regime attempts to access the international financial system through covert means. It makes it clear that these efforts are used to provide 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 designated groups.

Examples include:

- *Use of SDN-listed Central Bank of Iran (CBI) officials* – FinCEN highlights that CBI officials listed on the U.S. Department of the Treasury, Office of Foreign Assets Control's (OFAC) list of Specially Designated Nationals and Blocked Persons (SDN List) have historically facilitated the transfer of hard foreign currencies back to Iran and transacted for the benefit of the IRGC-QF and its beneficiaries. FinCEN advises financial institutions to exercise appropriate due diligence to avoid transacting with CBI officials, noting in particular that some counterparty financial institutions "may not be equipped to identify or address CBI officials' deceptive transactions."

- *Use of exchange houses* – As sanctions are reimposed on Iran following the lifting of the Joint Comprehensive Plan of Action (JCPOA), Iran can be expected to increase its use of third-country exchange houses or trading companies to act as money transmitters. Accordingly, FinCEN warns financial institutions to conduct proper due diligence when engaging with foreign exchange houses, including communicating with correspondent banks that hold accounts and facilitate transactions for such entities.
- *Use of front and shell companies to procure goods and services* – FinCEN highlights Iran's use of front and shell companies to procure goods and services, including those operating in the printing, dual-use equipment, and commercial aviation industries.
- *Use of deceptive practices related to shipping* – FinCEN notes deceptive practices used to hide the Iranian nexus to a transaction, including falsifying shipping documents to conceal docking in Iranian ports, as well as vessel ownership or operation transfers from SDNs to front companies or other agents. FinCEN advises that shipping companies may resort to the use of these or other evasive practices with the return of Iranian sanctions following the lifting of the JCPOA.
- *Use of precious metals* – FinCEN notes Iran's prior use of precious metals, such as gold, to evade U.S. sanctions and facilitate the sale of Iranian oil and other goods abroad, a practice FinCEN predicts will increase as the United States reimposes certain sanctions on Iran.
- *Use of virtual currency* – Individuals and businesses within Iran can access virtual currency platforms through the Internet. The advisory notes that OFAC's jurisdiction continues to apply to persons that facilitate or engage in online commerce, or process transactions using "digital currency." Financial institutions are thus responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, even if they involve digital currency.

Iran's AML/CFT Regime

In the advisory, FinCEN states that the Financial Action Task Force (FATF) has identified Iran as a jurisdiction with "systemic deficiencies" in its anti-money laundering and combatting the financing of terrorism (AML/CFT) regime. Noting that Iran failed to implement an action plan agreed to with the FATF in June 2016, FinCEN reiterates the need to apply enhanced due diligence measures to business relationships and transactions that involve Iranian persons and businesses.

Red Flags

The advisory additionally identifies red flags that financial institutions may use to help identify Iran's attempts to access the international financial system, noting that in some cases financial institutions should conduct additional diligence where appropriate. These red flags include:

I. Illicit activity by the CBI or its officials

- use of a personal account rather than central bank or government-owned accounts
- unusual wire transfers
- use of forged documents

II. Illicit activity through exchange houses

- use of multiple exchange houses
- multiple deposits from numerous individuals and entities that do not appear to match the account holder's profile or provided documentation

III. Use of procurement networks

- transactions with shell or front companies, as indicated by an affiliation with Iran or the Iran regime, opaque ownership structures, directors with obscure names, or business addresses that are residential or co-located with other companies
- suspicious declarations that are inconsistent with other information provided, such as transaction history or nature of business
- transactions directed to companies that operate in unrelated businesses

IV. Illicit procurement of aircraft part

- use of front companies and transshipment hubs to source aircraft parts
- misrepresenting to suppliers, dealers, brokers, reinsurers and other intermediaries that Iran sanctions no longer apply, or falsely claiming that an OFAC license has been obtained

V. Iran-related shipping companies' access to the financial system

- incomplete and falsified documentation, such as bills of lading and shipping invoices
- inconsistent documentation for vessels using key ports
- ship registration transferred from sanctioned persons

VI. Suspicious fund transfers

- lack of information regarding the origin of funds or information that does not match the customer's line of business
- unusual or unexplainable wire transfers that have no apparent connection to a customer's profile
- using funnel accounts, in which third parties deposit funds into the accounts of U.S.-based individuals with ties to Iran
- structuring transactions so as to avoid the currency transaction reporting threshold of $10,000
- use of unusually high volumes of gold

VII. Virtual currency

- logins from Iranian IP addresses or use of Iranian email accounts
- payments to/from an Iranian virtual currency entity
- peer-to-peer exchanges, including unexplained transfers into a customer account from multiple individual customers combined with transfers to, or from, virtual currency exchanges.

Financial Institutions and Iran

FinCEN concludes its advisory by reminding financial institutions of the broader sanctions and regulatory obligations pertinent to Iran, including OFAC's comprehensive Iranian sanctions program; AML regulatory obligations, as well as due diligence and suspicious activity reporting; and reporting requirements for U.S. banks under the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA).

Conclusion

FinCEN's advisory is a reminder of the U.S. and international regulatory prohibitions and obligations triggered by financial involvement with Iran, Iranian persons and those who do business with Iranian persons. As we have discussed in prior alerts, U.S. withdrawal from the JCPOA may usher in aggressive enforcement of U.S. sanctions regarding Iran by OFAC and the State Department. FinCEN's advisory extends that expectation to other U.S. financial regulatory regimes. These additional obligations increase the need for financial institutions, in particular, to engage in proper diligence and carefully scrutinize transactions to detect the potential illicit involvement of Iran, and to comply with relevant U.S. sanctions and financial controls.