FinCEN ADVISORY

FIN-2018-A004 **September 21, 2018**

Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies

On June 29, 2018, the Financial Action Task Force (FATF) updated its list of jurisdictions with strategic anti-money laundering and combatting the financing of terrorism (AML/CFT) deficiencies. The changes may affect U.S. financial institutions' obligations and risk-based approaches with respect to relevant jurisdictions.

As part of the FATF's listing and monitoring process to ensure compliance with its international AML/CFT standards, the FATF identifies certain jurisdictions as having strategic deficiencies in their AML/CFT regimes.[1] These jurisdictions are named in two documents: (1) the "FATF Public Statement," which identifies jurisdictions that are subject to the FATF's call for countermeasures and/or are subject to enhanced due diligence (EDD) due to their strategic AML/CFT deficiencies, and (2) "Improving Global AML/CFT Compliance: On-going Process," which identifies jurisdictions that the FATF has determined to have strategic AML/CFT deficiencies.[2] On June 29, 2018, the FATF updated both documents with the concurrence of the United States. Financial institutions should consider these changes when reviewing their obligations and risk-based policies, procedures, and practices with respect to the jurisdictions noted below.[3]

FATF "Public Statement":

- Democratic People's Republic of Korea (DPRK) and Iran

FATF "Improving Global AML/CFT Compliance: On-going Process":

- Remaining on list: Ethiopia, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, Yemen
- Added to list: Pakistan
- Removed from list: Iraq, Vanuatu

1. The FATF (www.fatf-gafi.org) is a 37-member intergovernmental body that establishes international standards to combat money laundering and counter the financing of terrorism and proliferation of weapons of mass destruction. The United States is a member of the FATF.

2. The FATF public identification of countries with strategic AML/CFT deficiencies is in response to the G-20 leaders' call for the FATF to reinvigorate its process for assessing countries' compliance with international AML/CFT standards. The G-20 leaders have consistently called for the FATF to issue regular updates on jurisdictions with strategic deficiencies. Specifically, within the FATF, the International Cooperation Review Group (ICRG) monitors and identifies countries with AML/CFT deficiencies. For more information on the ICRG procedures, please visit the FATF's website.

3. *See* 31 U.S.C. §§ 5318(h) and (i).

I. Jurisdictions that are subject to the FATF's call for countermeasures and/or are subject to EDD due to their strategic AML/CFT deficiencies

The FATF has stated that the following jurisdictions have strategic deficiencies in their AML/CFT regimes and has called upon its members and urged all jurisdictions to (1) impose countermeasures and/or (2) apply enhanced due diligence proportionate to the risks arising from the jurisdiction.

Please click on each jurisdiction for additional information.

A. Countermeasures:

Democratic People's Republic of Korea (DPRK)

B. Enhanced Due Diligence:

Iran

Review of Guidance Regarding the DPRK and Iran

Democratic People's Republic of Korea (DPRK)

The FATF calls on its members and other countries to apply countermeasures against the DPRK to protect the international financial system from money laundering and terrorist financing risks. The FATF Public Statement on the DPRK emphasizes the high risk of proliferation financing attributable to the DPRK, consistent with UN Security Council Resolutions (UNSCRs).[4] In particular, the FATF reaffirmed its call that jurisdictions terminate correspondent relationships with DPRK banks, which is required by UNSCR 2270. Financial institutions should be acutely aware of the financial provisions and comprehensive prohibitions contained in the UNSCRs imposing sanctions on the DPRK.

Among other prohibitions and restrictions, UNSCR 2321, adopted in 2016, states that member states shall expel individuals acting on behalf of or at the direction of a bank or financial institution of the DPRK. UNSCR 2321 also expresses concern that individuals from the DPRK are sent abroad to earn hard currency to fund the DPRK's nuclear and ballistic missile programs and also reiterates the concern that the DPRK may use bulk cash to evade UN measures. UNSCR 2321 instructed member states to close existing representative offices, subsidiaries, or banking accounts in the DPRK within 90 days of the adoption of the resolution (unless individually exempted by the 1718 Committee), and stated that member states shall prohibit public and private financial support within their territories or by persons or entities subject to their jurisdiction for trade with the DPRK.

4. Relevant UNSCRs include 2397 (December 2017), 2375 (September 2017), 2371 (August 2017), 2356 (June 2017), 2321 (November 2016), 2270 (March 2016), 2094 (March 2013), 2087 (January 2013), 1874 (June 2009), and 1718 (October 2006). *See* the UN Security Council Resolutions webpage for more information.

In addition to UN sanctions, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) maintains a robust sanctions program on North Korea through the North Korea Sanctions Regulations, which implements DPRK-related Executive Orders (E.O.) 13466, 13551, 13570, 13687, 13722, and 13810, the North Korea Sanctions and Policy Enhancement Act of 2016, and relevant provisions of the Countering America's Adversaries Through Sanctions Act of 2017.[5] Separately, under Non-Proliferation Sanctions such as Weapons of Mass Destruction Proliferators Sanctions Regulations,[6] as well as under E.O. 13382, OFAC administers sanctions on individuals and entities responsible for the proliferation of weapons of mass destruction (WMD), as well as their supporters, some of whom are North Korean or tied to North Korea and North Korean-related activity.[7] Collectively, these authorities prohibit U.S. persons, including U.S. financial institutions, from engaging in nearly all transactions involving the DPRK.[8] These sanctions are a direct response to the DPRK's ongoing development of WMD and their means of delivery; the launching of intercontinental ballistic missiles; nuclear tests; human rights abuses and censorship; destructive, coercive cyber-related actions; involvement in money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking, in continued violation of the UNSCRs.[9]

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with E.O. 13810 (September 2017).[10] The E.O. provides the Secretary of the Treasury, in consultation with the Secretary of State, additional tools to disrupt a broad range of DPRK-related activity, to include North Korea's ability to fund its WMDs and ballistic missile programs. Specifically, E.O. 13810: (1) establishes several new designation criteria; (2) prohibits vessels and

5. *See* U.S. Department of the Treasury's Resource Center for North Korea Sanctions, 22 U.S.C. § 9201 et seq., and Public Law 115-44.

6. *See* 31 CFR Part 544.

7. *See* Executive Order 13382—Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters.

8. Further information about these sanctions is available on OFAC's Resource Center for DPRK Sanctions and the OFAC Recent Actions web page. OFAC's sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in most transactions involving the DPRK, the Government of North Korea, and the Korean Workers' Party. OFAC recently took a series of sanctions actions related to the DPRK, including actions pursuant to Executive Orders 13722 and 13810 on September 13, 2018 and on September 6, 2018 actions pursuant to Executive Order 13810. OFAC also took sanctions actions related to DPRK on August 21, 2018 and August 15, 2018, as well as additional sanctions actions on August 3, 2018, pursuant to Executive Orders 13687, 13382, and 13722. OFAC previously took sanctions actions related to the DPRK pursuant to Executive Orders 13810 and 13722 on February 23, 2018. OFAC also issued DPRK-related sanctions pursuant to Executive Orders 13687, 13722, and 13810 on January 24, 2017. OFAC took other DPRK-related sanctions actions pursuant to Executive Orders 13810 and 13722 on November 21, 2017. OFAC imposed other DPRK-related actions pursuant to Executive Orders 13687 and 13722 on October 26, 2017, Executive Order 13810 on September 26, 2017, and Executive Orders 13382 and 13722 on August 22, 2017. OFAC took other DPRK-related sanctions pursuant to one or more of these same authorities on December 26, 2017, June 29, 2017, June 1, 2017, March 31, 2017, December 2, 2016, and September 26, 2016. On November 20, 2017, the United States designated the DPRK a state sponsor of terrorism.

9. *See* Executive Orders 13810 (September 20, 2017), 13687 (January 2, 2015), and 13551 (August 30, 2010).

10. *See* U.S. Department of the Treasury's Resource Center for September 21, 2017 actions relating to North Korea and Remarks by Secretary Mnuchin on President Trump's Executive Order on North Korea.

aircraft that have called or landed at a port or place in North Korea in the previous 180 days, and vessels that engaged in a ship-to-ship transfer with such a vessel in the previous 180 days, from entering the United States; (3) provides authority to block any funds transiting accounts with links to North Korea that come within the United States or in the possession of a United States person; and (4) provides authority to impose sanctions on a foreign financial institution (FFI) that knowingly conducts or facilitates on or after September 21, 2017 (i) any significant transaction on behalf of person blocked under the DPRK-related E.O.s or persons blocked under E.O. 13382 for North Korea-related activities or (ii) any significant transaction in connection with trade with North Korea. The sanctions applicable to FFIs can be restrictions on correspondent or payable-through accounts or full blocking sanctions.[11]

Since the issuance of E.O. 13810, OFAC has designated entities and individuals involved in North Korea's illicit shipping and transportation activities, trading companies, and financial and banking representatives, and identified multiple vessels as blocked property.[12] On July 23, 2018, OFAC issued a joint advisory[13] with the U.S. Department of State and the U.S. Department of Homeland Security to alert all U.S. persons to the sanctions evasion tactics used by North Korea that could expose businesses – including manufacturers, buyers, and service providers – to supply chain sanctions compliance risks under U.S. or United Nations sanctions authorities. Earlier, on February 23, 2018, with the U.S. Department of State and the U.S. Coast Guard, OFAC issued a North Korea Sanctions Advisory on sanctions risks related to North Korea's shipping practices, to alert persons globally of North Korea's deceptive shipping practices to evade U.S. and UN sanctions.[14]

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. On November 9, 2016, the Financial Crimes Enforcement Network (FinCEN) issued a final rule, effective December 9, 2016, imposing the fifth special measure against the DPRK, consistent with the FinCEN's finding that the DPRK is a jurisdiction of "primary money laundering concern" under Section 311 of the USA PATRIOT Act.[15] The fifth special measure, codified at 31 U.S.C. 5318A(b)(5), allows FinCEN to prohibit or impose conditions on the opening or maintaining of correspondent or payable-through accounts for the identified jurisdiction by U.S. financial institutions. The notice of finding and the final rule stressed that the North Korean government continues to use state-controlled financial institutions and front companies to conduct surreptitiously illicit international financial transactions, some of which support the proliferation of WMD and the development of ballistic missiles. The final rule prohibits covered financial institutions from opening or maintaining in the U.S. correspondent accounts for, or

11. *See* OFAC's FAQs.

12. *See* Executive Order 13810 (September 20, 2017).

13. *See* U.S. Department of the Treasury's Resource Center.

14. *See* U.S. Department of the Treasury's Press Release, Treasury Announces Largest North Korean Sanctions Package Targeting 56 Shipping and Trading Companies and Vessels to Further Isolate Rogue Regime.

15. *See* U.S. Department of the Treasury's Resource Center and 81 FR 78715 (November 9, 2016). FinCEN issued the notice of finding and notice of proposed rulemaking (NPRM) on June 2, 2016 (81 FR 35441) and June 3, 2016 (81 FR 35665).

on behalf of, North Korean banking institutions and requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against the use of such accounts to process transactions involving North Korean financial institutions.

On November 2, 2017, FinCEN issued a final rule, effective December 8, 2017, under Section 311 of the USA PATRIOT Act, that severed the Bank of Dandong, a Chinese bank that has acted as a conduit for illicit North Korean financial activity, from the U.S. financial system. The final rule stressed that the Bank of Dandong has acted as a conduit for North Korea to access the U.S. and international financial systems, including the facilitation of millions of dollars of transactions for companies involved in North Korea's WMD and ballistic missile programs.

The Bank of Dandong has also facilitated financial activity for North Korean entities designated by the United States and listed by the UN for proliferation of WMDs, as well as for front companies acting on their behalf. The final rule: a) prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or on behalf of, the Bank of Dandong; b) requires covered financial institutions to take reasonable steps not to process a transaction for the correspondent account of a foreign bank in the United States if such a transaction involves the Bank of Dandong; and c) requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Bank of Dandong.[16]

FinCEN also issued an advisory in tandem with the Bank of Dandong Section 311 Final Rule to further alert financial institutions to schemes commonly used by North Korea to evade U.S. and U.N. sanctions, launder funds, and finance the North Korean regime's weapons programs.[17]

Iran

The FATF continues to call upon its members and all jurisdictions to apply enhanced due diligence measures to protect against the terrorist financing risk emanating from Iran and the threat this risk poses to the international financial system. In addition to keeping Iran on its Public Statement, during its June 2018 Plenary, the FATF expressed disappointment "with Iran's failure to implement its action plan to address its significant AML/CFT deficiencies" as Iran has not addressed nine out of 10 requirements in its AML/CFT action plan.[18] The FATF again

16. *See* U.S. Department of the Treasury's Press Release, FinCEN Further Restricts North Korea's Access to the U.S. Financial System and Warns U.S. Financial Institutions of North Korean Schemes; Press Release, Treasury Finalizes Action to Further Restrict North Korea's Access to the U.S. Financial System; and FinCEN's Imposition of Special Measure against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern, 82 FR 51758 (November 8, 2017).

17. *See* FinCEN Advisory FIN-2017-A008, "Advisory on North Korea's Use of the International Financial System" (November 2017). In addition, FinCEN has three other advisories relating to the DPRK: FIN-2013-A005, "Update on the Continuing Illicit Finance Threat Emanating from North Korea" (July 2013); FIN-2009-A002, "North Korea Government Agencies' and Front Companies' Involvement in Illicit Financial Activities" (June 2018); and FinCEN Advisory – Issue 40, "Guidance to Financial Institutions on the Provisions of Banking Services to North Korean Government Agencies and Associated Front Companies Engaged in Illicit Activities" (December 2005).

18. *See* FATF's June 2018 Public Statement.

highlighted these major deficiencies in Iran's AML/CFT regime and 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 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 value."[19]

The FATF reiterated its continued concern with the terrorist financing risk emanating from Iran and called upon its members and urged all jurisdictions to continue to advise their financial institutions to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from Iran. The FATF will decide upon further action in October 2018, if Iran has not enacted the necessary amendments to its AML and CFT laws and ratified the Terrorist Financing and Palermo Conventions.

Treasury has consistently underscored the risks of conducting business with entities associated with Iran.[20] Iran continues to use deceptive tactics including front and shell companies to exploit markets in numerous countries to fund its nefarious activities. Iran's tactics include forging documents, obfuscating data, and hiding illicit activities under official cover of government entities, among many others. For instance, Treasury sanctioned high-level officials of the Central Bank of Iran (CBI), including the CBI Governor at the time, for collaborating with the Islamic Revolutionary Guard Corps - Qods Force (IRGC-QF) to conceal the movement of millions of dollars to fund Hizballah. In addition, Treasury targeted a currency exchange network that Iran was using in Iran and the United Arab Emirates to procure and move millions of dollars to the IRGC-QF, which the CBI also enabled. To combat Iran's malign activities, including its efforts to deceive the international business community, since February 2017, OFAC has designated 146 Iran-related persons in 18 rounds of

19. Ibid.

20. In addition to OFAC sanctions, FinCEN has issued numerous advisories related to Iran., *see* FinCEN Advisory FIN-2018-A002, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (April 2018); FinCEN Advisory FIN-2010-A008, "Update on the Continuing Illicit Finance Threat Emanating from Iran" (June 2010); FinCEN Advisory FIN-2008-A002, "Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity" (March 2008); and FinCEN Advisory FIN-2007-A001, "Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity" (October 2007).

sanctions for Iran's support for terrorism, WMD proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses.[21] Additionally, financial institutions should be familiar with the requirements and prohibitions contained in UNSCR 2231 related to Iran.[22]

The continued suspension of countermeasures against Iran keeps Iran on the FATF Public Statement. This action does not remove or alter any obligation of U.S. persons, including financial institutions, regarding a broad range of restrictions and prohibitions on engaging in transactions with or involving Iran given the large number of illicit finance risks associated with Iran, including money laundering, terrorist financing, human rights abuses, and the financing of Iran's ballistic missile program.

Review of Guidance on Section 312 Obligations Relating to the DPRK and Iran

Financial institutions must comply with the extensive U.S. restrictions and prohibitions against opening or maintaining any correspondent accounts, directly or indirectly, with foreign banks licensed by the DPRK or Iran.

In the case of DPRK, existing U.S. sanctions and the FinCEN December 2016 final rule imposing the fifth special measure against the DPRK already prohibit any such correspondent account relationships, superseding the Section 312 obligations.

In the case of Iran, the Government of Iran and Iranian financial institutions remain persons whose property and interests in property are blocked under E.O. 13599 and section 560.211 of the Iranian Transactions and Sanctions Regulations. U.S. financial institutions and other U.S. persons continue to be broadly prohibited under the Iranian Transactions and Sanctions Regulations from engaging in transactions or dealings with Iran, the Government of Iran, and Iranian financial institutions, including opening or maintaining correspondent accounts for Iranian financial institutions; these sanctions impose obligations on U.S. persons that go beyond the obligations imposed under Section 312.

21. On August 6, 2018, E.O. 13846 reimposed certain sanctions with respect to Iran. This E.O. supports the United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the initial 90-day wind-down period. The 180-day wind-down period will end on November 4, 2018. Consult OFAC's FAQ concerning E.O. 13846 and the reimposition of sanctions that occurred by August 6, 2018. In addition to sanctions reimposed by E.O., 13846, OFAC issued Iran-related designations on September 14, 2018, July 9, 2018, May 30, 2018, May 24, 2018, May 22, 2018, May 17, 2018, May 15, 2018, May 10, 2018, March 23, 2018, January 12, 2018, January 4, 2018, November 20, 2017, and October 13, 2017. Furthermore, OFAC previously issued Iran-related designations associated with Iran's ballistic missile program on July 28, 2017, July 18, 2017 (in conjunction with those issued by the U.S. Department of State and in coordination with the U.S. Department of Justice's release of information involving a related criminal enforcement action), September 14, 2017, May 17, 2017, April 13, 2017, and February 3, 2017. Consult OFAC's Iran Sanctions web page and the OFAC Recent Actions web page for more detailed information about the sanctions included in this footnote.
22. UNSCR 2231 (July 2015) revises UN sanctions and other prohibitions, including financial prohibitions, concerning Iran; the UN maintains a list of individuals and entities subject to targeted financial sanctions.

Reminder of General 312 Obligations

As a general matter, FinCEN reminds U.S. financial institutions of their duty to apply enhanced due diligence when maintaining correspondent accounts for foreign banks operating under a banking license issued by a country (1) designated as non-cooperative with respect to international anti-money laundering principles or procedures, by an intergovernmental group or organization of which the United States is a member, and with which designation the U.S. representative to the group or organization concurs, or (2) that has been designated as warranting special measures under Section 311.[23] The regulations implementing the Bank Secrecy Act, as amended by the USA PATRIOT Act, requires covered financial institutions ensure that their enhanced due diligence programs include, at a minimum, steps to:

- Conduct enhanced scrutiny of correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable law and regulation;
- Determine whether the foreign bank for which the correspondent account is established or maintained in turn maintains correspondent accounts for other foreign banks that use the foreign correspondent account established or maintained by the covered financial institution and, if so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign bank's correspondent accounts for other foreign banks, including, as appropriate, the identity of those foreign banks; and
- Determine, for any correspondent account established or maintained for a foreign bank whose shares are not publicly traded, the identity of each owner of the foreign bank and the nature and extent of each owner's ownership interest.[24]

II. Jurisdictions identified by the FATF as having strategic AML/CFT deficiencies

The FATF publicly identifies jurisdictions with strategic AML/CFT regime deficiencies for which the jurisdictions have developed an action plan with the FATF. Consequently, these jurisdictions are included in the following list of jurisdictions with strategic AML/CFT deficiencies, as described in the FATF's "Improving Global AML/CFT Compliance: On-going Process."

Please click on each jurisdiction for additional information.

Ethiopia, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen

23. *See* 31 U.S.C. § 5318(i); 31 CFR §§ 1010.610(b) and (c) (Enhanced Due Diligence obligations for correspondent accounts established, maintained, administered or managed in the United States for certain foreign banks).

24. Ibid.

Summary of Changes to this List

Countries Removed from the List

- Iraq is no longer subject to the FATF's monitoring process under its ongoing global AML/CFT compliance process. The FATF welcomes Iraq's significant progress in improving its AML/CFT regime and notes that Iraq has established the legal and regulatory framework to meet the commitments in its action plan regarding the strategic deficiencies that the FATF identified in October 2013. Iraq will work with Middle East and North Africa FATF (MENAFATF) to improve further its AML/CFT regime.

- Vanuatu is no longer subject to the FATF's monitoring process under its ongoing global AML/CFT compliance process. The FATF welcomes Vanuatu's significant progress in improving its AML/CFT regime and notes that Vanuatu has established the legal and regulatory framework to meet the commitments in its action plan regarding the strategic deficiencies that the FATF identified in February 2016. Vanuatu will work with the Asia Pacific Group on Money Laundering (APG) to improve further its AML/CFT regime.

Countries Added to the List

- Pakistan has been added to the list[25] and will undergo monitoring by FATF's International Co-operation Review Group (ICRG) based on the specific AML/CFT deficiencies highlighted by the FATF. Pakistan made a commitment to work with the FATF and APG to strengthen its AML/CFT regime and to address its strategic counter-terrorist financing-related deficiencies, "including by (1) demonstrating that TF risks are properly identified, assessed, and that supervision is applied on a risk-sensitive basis; (2) demonstrating that remedial actions and sanctions are applied in cases of AML/CFT violations, and that these actions have an effect on AML/CFT compliance by financial institutions; (3) demonstrating that competent authorities are cooperating and taking action to identify and take enforcement action against illegal money or value transfer services (MVTS); (4) demonstrating that authorities are identifying cash couriers and enforcing controls on illicit movement of currency and understanding the risk of cash couriers being used for TF; (5) improving inter-agency coordination including between provincial and federal authorities on combating TF risks; (6) demonstrating that law enforcement agencies are identifying and investigating the widest range of TF activity and that TF investigations and prosecutions target designated persons and entities, and persons and entities acting on behalf or at the direction of the designated person or entities; (7) demonstrating that TF prosecutions result in effective, proportionate and dissuasive sanctions and enhancing the capacity and support for prosecutors and the judiciary; (8) demonstrating effective implementation of targeted financial sanctions (supported by a comprehensive legal obligation) against all 1267 and 1373 designated terrorists and those acting for or on their behalf, including preventing the raising and moving of funds,

25. *See* "Improving Global AML/CFT Compliance: On-going Process - 29 June 2018."

identifying and freezing assets (movable and immovable), and prohibiting access to funds and financial services; (9) demonstrating enforcement against TFS [Targeted Financial Sanctions] violations including administrative and criminal penalties and provincial and federal authorities cooperating on enforcement cases; and (10) demonstrating that facilities and services owned or controlled by designated persons are deprived of their resources and the usage of the resources."[26]

Review of Guidance Regarding Jurisdictions Having Strategic AML/CFT deficiencies

U.S. financial institutions also should consider the risks associated with the AML/CFT deficiencies of the countries identified under this section (Ethiopia, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen).[27] With respect to these jurisdictions, U.S. financial institutions are reminded of their obligations to comply with the due diligence obligations for FFIs under 31 CFR § 1010.610(a) in addition to their general obligations under 31 U.S.C. § 5318(h) and its implementing regulations.[28] As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for FFIs, 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. Such reasonable steps should not, however, put into question a financial institution's ability to maintain or otherwise continue appropriate relationships with customers or other financial institutions, and should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions. FinCEN also reminds financial institutions of previous interagency guidance on providing services to foreign embassies, consulates, and missions.[29]

26. Ibid.

27. This Advisory updates previous FATF-related guidance on identified jurisdictions with AML/CFT deficiencies. Additional FinCEN guidance on Syria includes FIN-2013-A002 and FIN-2011-A010 as well as FinCEN's guidance on the Commercial Bank of Syria; *see* FIN-2011-A013.

28. *See,* generally, 31 CFR § 1010.210: Anti-money laundering programs. Specific AML Program obligations are prescribed in 31 CFR §§ 1020.210 (Banks), 1021.210 (Casinos and Card Clubs), 1022.210 (Money Services Businesses), 1023.210 (Brokers or Dealers in Securities), 1024.210 (Mutual Funds), 1025.210 (Insurance Companies), 1026.210 (Futures Commission Merchants and Introducing Brokers in Commodities), 1027.210 (Dealers in Precious Metals, Precious Stones, or Jewels), 1028.210 (Operators of Credit Card Systems), 1029.210 (Loan or Finance Companies), and 1030.210 (Housing Government Sponsored Enterprises).

29. *See* Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates, and Missions," March 24, 2011 and Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, "Interagency Advisory: Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies, and Foreign Political Figures," June 15, 2004.

Review of General Guidance

AML Program Risk Assessment: For the jurisdictions that were removed from the FATF listing and monitoring process (Iraq and Vanuatu), financial institutions should take the FATF's decisions and the reasons behind the delisting into consideration when assessing risk, consistent with their obligations under 31 CFR §§ 1010.610(a) and 1010.210.[30]

Suspicious Activity Reports (SARs): If a financial institution knows, suspects, or has reason to suspect that a transaction involves funds derived from illegal activity or that a customer has otherwise engaged in activities indicative of money laundering, terrorist financing, or other violation of federal law or regulation, the financial institution must file a SAR.[31]

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 in the SAR narrative and in SAR field 35(z) (Other Suspicious Activity-Other) by including the following key term:**

"June 2018 FATF FIN-2018-A004"

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

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing as well as money laundering and terrorist financing. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, OFAC designation efforts, and the overall security and stability of the U.S. financial system.[32]

30. *Supra* note 17.
31. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
32. For example case studies, see SAR Activity Review, Issue 19, beginning on page 25, and Law Enforcement Case Examples.

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. ***Financial institutions wanting to report suspicious transactions that may 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.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.