FinCEN ADVISORY

FIN-2019-A001 March 8, 2019

Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies

On February 22, 2019, 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.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to inform financial institutions of updates to the FATF list of jurisdictions with strategic AML/CFT deficiencies. Financial institutions should be aware of these changes, which may affect their obligations and risk-based approaches with respect to these jurisdictions. The advisory also reminds financial institutions of the status and obligations involving these jurisdictions, in particular the Democratic People's Republic of Korea (DPRK) and Iran.

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 enhanced due diligence (EDD) because of 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 February 22, 2019, 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]

1. The FATF (www.fatf-gafi.org) is a 38-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's public identification of jurisdictions with strategic AML/CFT deficiencies is in response to the G20 leaders' call for the FATF to reinvigorate its process for assessing jurisdictions' compliance with international AML/CFT standards. The G20 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 jurisdictions 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).

FATF Public Statement:

- DPRK and Iran

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

- Remaining on list: The Bahamas, Botswana, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen
- Added to list: Cambodia

Jurisdictions that are Subject to the FATF's Call for Countermeasures and/or 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 EDD proportionate to the risks arising from the jurisdiction.

Countermeasures

DPRK

Enhanced Due Diligence

Iran

Review of Guidance Regarding the DPRK and Iran

DPRK

FATF Actions: Public Statement on the DPRK

The FATF issued the following public statement concerning the DPRK:

"The FATF remains concerned by the DPRK's failure to address the significant deficiencies in its anti-money laundering and combating the financing of terrorism (AML/CFT) regime and the serious threats they pose to the integrity of the international financial system. The FATF urges the DPRK to immediately and meaningfully address its AML/CFT deficiencies. Further, the FATF has serious concerns with the threat posed by the DPRK's illicit activities related to the proliferation of weapons of mass destruction (WMD) and its financing.

The FATF reaffirms its 25 February 2011 call on its members and urges all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. In addition to enhanced scrutiny, the FATF further calls on its members and urges all jurisdictions to

apply effective counter-measures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions, to protect their financial sectors from money laundering, financing of terrorism and WMD proliferation financing (ML/FT/PF) risks emanating from the DPRK. Jurisdictions should take necessary measures to close existing branches, subsidiaries and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks, where required by relevant UNSC resolutions."[4]

United Nations: Related Sanctions on the DPRK

The United Nations (UN) has adopted a number of resolutions implementing economic and financial sanctions, as well as other prohibitions and restrictions with respect to the DPRK. Member States are bound by the provisions of these United Nations Security Council Resolutions (UNSCRs).[5] Most recently, UNSCR 2397 (2017) called upon Member States to redouble efforts to implement measures in all DPRK-related UNSCRs, and certain provisions of these resolutions are especially relevant to financial institutions. For example, UNSCR 2270 (2016) requires Member States to prohibit financial institutions from establishing new joint ventures and from taking an ownership interest in or establishing or maintaining correspondent relationships with DPRK banks without advance approval from the UN.

Financial institutions should also be aware of UNSCR 2321 (2016), which states that Member States must 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 it reiterates the concern that the DPRK may use bulk cash to evade UN measures. UNSCR 2321 also instructs 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 states 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.

United States: Related Sanctions, Prohibitions, and Other Measures Concerning the DPRK

In addition to UN sanctions, the U.S. Department of the Treasury's (Treasury) Office of Foreign Assets Control (OFAC) maintains a robust sanctions program on North Korea[6] through the North Korea Sanctions Regulations, 31 C.F.R. Part 510 (NKSR), which implements DPRK-related Executive Orders (E.O.) 13466, 13551, 13570, 13687, 13722, and 13810; as well as the North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA), as amended by Title III of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA).[7] The NKSR and Executive orders generally prohibit most direct or indirect commercial, financial, or

4. Financial Action Task Force Public Statement – February 2019, (February 22, 2019).
5. 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 United Nations Security Council Resolutions web page for more information.
6. The DPRK is also referred to as North Korea.
7. *See* Treasury's Resource Center for North Korea Sanctions, 22 U.S.C. § 9201 et seq., and Public Law 115-44.

trade transactions by U.S. persons[8] or within the United States that involve North Korea or the property or interests in property of any individual or entity designated pursuant to the NKSR program unless authorized by OFAC or exempted by statute.[9] Separately, under the Weapons of Mass Destruction Proliferators Sanctions Regulations,[10] issued pursuant to E.O. 13382, OFAC administers sanctions on individuals and entities responsible for the proliferation of WMD, as well as their supporters, some of whom are North Korean or tied to North Korea and North Korean-related activity.[11] These sanctions are a direct response to the DPRK's ongoing development of WMD and their means of delivery; 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; and continued violations of UNSCRs.[12]

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with E.O. 13810 (September 2017).[13] 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 WMD and ballistic missile programs. Specifically, E.O. 13810: (1) establishes several new designation criteria; (2) prohibits vessels and 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 any 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.[14]

8. The term *United States person* or *U.S. person* means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States. 31 C.F.R.§ 510.326.

9. Further information about these sanctions is available at OFAC's Resource Center for DPRK Sanctions and the OFAC Recent Actions web page. OFAC recently took a series of sanctions actions related to the DPRK, including actions on December 10, 2018 and November 19, 2018. Previously, OFAC took sanctions actions related to the DPRK on October 25, 2018, October 4, 2018, September 13, 2018, September 6, 2018, August 21, 2018, August 15, 2018, August 3, 2018, February 23, 2018, January 24, 2018, November 21, 2017, October 26, 2017, September 26, 2017, August 22, 2017, December 26, 2017, June 29, 2017, June 1,2017, March 31, 2017, December 2, 2016, and September 26, 2016.

10. *See* 31 CFR Part 544.

11. *See* Executive Order 13382 (June 29, 2005).

12. *See* Executive Orders 13810 (September 21, 2017), 13687 (January 2, 2015), and 13551 (August 30, 2010).

13. *See* 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 (September 21, 2017).

14. *See* OFAC's Frequently Asked Questions (FAQs).

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.[15] On August 3, 2018, OFAC designated Russian-registered Agrosoyuz Commercial Bank pursuant to Section 4 of E.O. 13810 for knowingly conducting or facilitating a significant transaction on behalf of a representative of U.S.- and UN-designated Foreign Trade Bank, North Korea's primary foreign exchange bank.[16] On July 23, 2018, OFAC issued a joint advisory with the U.S. Department of State and the U.S. Department of Homeland Security to alert businesses, to include U.S. and foreign businesses, to the sanctions evasion tactics used by North Korea that could expose them—including manufacturers, buyers, and service providers—to supply chain sanctions compliance risks under U.S. or UN sanctions authorities.[17] 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.[18]

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. In November 2016, pursuant to Section 311 of the USA PATRIOT Act, FinCEN issued a final rule prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, North Korean banking institutions and requiring 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.[19] FinCEN noted that the North Korean government continues to use state-controlled financial institutions and front companies to conduct illicit international financial transactions, some of which support the proliferation of WMD and the development of ballistic missiles.[20]

In November 2017, FinCEN also prohibited U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, Bank of Dandong, and required those 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.[21] In promulgating the regulation, FinCEN found that the Chinese bank has acted as a conduit for illicit North Korean financial activity to access the U.S. and international financial systems, including the facilitation of millions of dollars of transactions for companies involved in

15. *See* Executive Order 13810 (September 21, 2017).
16. *See* Treasury's Press Release, "Treasury Targets Russian Bank and Other Facilitators of North Korean United Nations Security Council Violations" (August 3, 2018).
17. *See* Treasury's Resource Center, "Publication of North Korea Supply Chain Advisory" (July 23, 2018).
18. *See* Treasury's Press Release, "Treasury Announces Largest North Korean Sanctions Package Targeting 56 Shipping and Trading Companies and Vessels to Further Isolate Rogue Regime" (February 23, 2018).
19. 31 C.F.R. § 1010.659.
20. *Id.*
21. 31 C.F.R. § 1010.660.

North Korea's WMD and ballistic missile programs. Further, FinCEN found that 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 WMD, as well as for front companies acting on their behalf.[22]

On November 2, 2017, FinCEN also issued an advisory to further alert financial institutions to schemes commonly used by North Korea to evade U.S. and UN sanctions, launder funds, and finance the North Korean regime's weapons programs.[23]

Iran

FATF Actions: Public Statement on Iran

The FATF issued a public statement concerning Iran. Excerpts from the statement are provided below. To read the public statement in its entirety, please see the Financial Action Task Force's Public Statement – February 2019.

"In February 2019, the FATF noted that there are still items [of Iran's Action Plan that are] not completed and Iran should fully address: (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 operational independence of the Financial Intelligence Unit and clarifying that the submission of [Suspicious Transaction Reports] STRs for attempted [Terrorist Financing] TF-related transactions are covered under Iran's legal framework; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF Conventions and clarifying the capability to provide mutual legal assistance; and (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information. …

If by June 2019, Iran does not enact the remaining legislation in line with FATF Standards, then the FATF will require increased supervisory examination for branches and subsidiaries of financial institutions based in Iran. The FATF also expects Iran to continue to progress with enabling regulations and other amendments.

Iran will remain on the FATF Public Statement until the full Action Plan has been completed. Until Iran implements the measures required to address the deficiencies identified with respect to countering terrorism-financing in the Action Plan, the FATF will remain concerned with the terrorist financing risk emanating from Iran and the threat this poses to the international financial

22. *Id*.

23. *See* FIN-2017-A008, "Advisory on North Korea's Use of the International Financial System" (November 2017). In addition, FinCEN has issued 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 2009); 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).

system. The FATF, therefore, calls on its members and urges all jurisdictions to continue to advise their financial institutions to apply enhanced due diligence with respect to business relationships and transactions with natural and legal persons from Iran, consistent with FATF Recommendation 19, including: (1) obtaining information on the reasons for intended transactions; and (2) conducting enhanced monitoring of business relationships by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination."[24]

United Nations: Related Sanctions on Iran

Financial institutions should be familiar with the requirements and prohibitions contained in UNSCR 2231 related to Iran.[25]

United States: Related Sanctions, Prohibitions, and other Measures Related to Iran

The United States has consistently underscored the risks of conducting business with entities associated with Iran. Iran continues to use deceptive tactics, including front and shell companies to exploit markets in numerous jurisdictions, 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. On October 11, 2018, FinCEN issued an advisory outlining the deceptive practices the Iranian regime employs to access the international financial system with the intention of furthering its illicit and malign activities.[26]

On November 5, 2018, the United States fully re-imposed the sanctions on Iran that had been lifted or waived under The Joint Comprehensive Plan of Action (JCPOA). These sanctions target critical sectors of Iran's economy, such as the energy, shipping, shipbuilding, and financial sectors. The United States is engaged in a campaign of maximum financial pressure on the Iranian regime and intends to enforce aggressively these sanctions that have come back into effect. As part of the re-imposition of U.S. sanctions, in its largest ever single-day action targeting the Iranian regime, OFAC sanctioned more than 700 individuals, entities, aircraft, and vessels on November 5, 2018. This action was a critical part of the re-imposition of the remaining U.S. sanctions that were lifted or waived in connection with the JCPOA.[27]

---

24. Financial Action Task Force Public Statement – February 2019, (February 22, 2019).

25. UNSCR 2231 (July 2015) revises UN sanctions and other prohibitions, including financial prohibitions, concerning Iran. Financial institutions should be aware that the UN maintains a list of individuals and entities subject to targeted financial sanctions.

26. *See* FIN-2018-A006, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System" (October 2018). FinCEN has issued numerous advisories related to Iran. *See* FIN-2018-A007, " "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (October 2018); FIN-2018-A004 FIN-2018-A004, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (September 2018); FIN-2018-A002, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies" (April 2018); FIN-2010-A008, "Update on the Continuing Illicit Finance Threat Emanating from Iran" (June 2010); FIN-2008-A002, "Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity" (March 2008); and FIN- 2007-A001, "Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian Activity" (October 2007).

27. *See* The U.S. Department of the Treasury's Resource Center, Iran Sanctions page for more information and Treasury's Press Release "U.S. Government Fully Re-Imposes Sanctions on the Iranian Regime as Part of Unprecedented U.S. Economic Pressure Campaign."

Additionally, OFAC administers and enforces a comprehensive trade embargo against Iran as set forth in the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. Part 560; Executive orders, issued under the authority of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-06; and other statutes. The ITSR generally prohibits most direct or indirect commercial, financial, or trade transactions with Iran by U.S. persons or within the United States, unless authorized by OFAC or exempted by statute.[28]

To combat Iran's malign activities, including its efforts to deceive the international business community, OFAC has issued 24 rounds of sanctions since February 2017, targeting 927 Iran-related persons, aircraft, and vessels in connection with a range of activities, including Iran's support for terrorism, ballistic missile program, WMD proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses.[29] Most recently, on February 13, 2019, OFAC designated Iran's New Horizon Organization for providing support to the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) along with four Iranian individuals affiliated with New Horizon Organization. That same day, OFAC sanctioned Iran-based Net Peygard Samavat Company and six associated individuals who were involved in a malicious cyber campaign to gain access to and implant malware on the computer systems of current and former U.S. counterintelligence agents.[30]

Review of Guidance on Section 312 Obligation 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 the DPRK, existing U.S. sanctions and FinCEN regulations already prohibit any such correspondent account relationships, superseding the Section 312 obligations.

28. The ITSR also prohibit entities owned or controlled by a United States person and established or maintained outside the United States ("U.S.-owned or -controlled foreign entities") from knowingly engaging in any transaction directly or indirectly with the Government of Iran or any person subject to the jurisdiction of the Government of Iran that would be prohibited by the ITSR if the transaction were engaged in by a U.S. person or in the United States.

29. On November 5, 2018, the United States re-imposed the sanctions that were lifted or waived under the JCPOA, and OFAC posted to its website additional frequently asked questions (FAQs) that provide guidance on the sanctions that have been re-imposed, amended several FAQs, and archived outdated FAQs. In addition to sanctions re-imposed by E.O. 13846, OFAC issued Iran-related designations on February 13, 2019, January 24, 2019, October 16, 2018, 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.

30. *See* Treasury's Press Release "Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons" (February 2019).

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 ITSR. U.S. financial institutions and other U.S. persons continue to be broadly prohibited under the ITSR 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.

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 is the subject of special measures pursuant to Section 311 of the USA PATRIOT Act.[31]

The regulations implementing the Bank Secrecy Act, as amended by the USA PATRIOT Act, require covered financial institutions to ensure that their enhanced due diligence programs include, at a minimum, steps to:

- Conduct enhanced scrutiny of such 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 such 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.[32]

31. Referring to 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).

32. *Id*.

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 publication entitled "Improving Global AML/CFT Compliance: On-going Process."

- The Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen.

Summary of Changes

Jurisdiction Added to the List

- Cambodia has been added to the list due to the lack of effective implementation of its AML/CFT framework. Cambodia has made a high-level political commitment to work with the FATF and the relevant FATF Style Regional Body (the Asia Pacific Group) to strengthen the effectiveness of its AML/CFT regime, and to address any related technical deficiencies.

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 jurisdictions identified under this section (The Bahamas, Botswana, Cambodia, Ethiopia, Ghana, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, and Yemen).[33] With respect to these jurisdictions, U.S. covered 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.[34] 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

33. This advisory updates previous FATF-related guidance on identified jurisdictions with AML/CFT deficiencies. Additional FinCEN advisories on Syria include FIN-2013-A002 and FIN-2011-A010 as well as FIN-2011-A013, FinCEN's advisory on the Commercial Bank of Syria.

34. *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).

report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States. Furthermore, money services businesses (MSBs) are reminded of their parallel requirements with respect to foreign agents or foreign counterparties, as described in FinCEN Interpretive Release 2004-1, which clarifies that an MSB's AML Program requires the MSB to establish adequate and appropriate policies, procedures, and controls commensurate with the risk of money laundering and the financing of terrorism posed by their relationship with foreign agents or foreign counterparties (69 FR 239, Dec.14, 2004). Additional information on these parallel requirements (covering both domestic and foreign agents, and foreign counterparts) may be found in FinCEN's *Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring*.[35] 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.[36]

AML Program Risk Assessment: For the jurisdictions that were removed from the FATF listing and monitoring process, 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.

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.

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. **FinCEN requests financial institutions only use the updated mandatory SAR form (as of February 1, 2019) and reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) by including the following key term: "February 2019 FATF FIN-2019-A001"** to indicate a connection between the suspicious activity being reported and the jurisdictions and activities highlighted in this advisory. SAR reporting, in conjunction

35. *See* FIN-2016-G001 (March 11, 2016).

36. *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.

with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing, other financial crimes associated with foreign and domestic political corruption, 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.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at 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.

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.