

FIN-2018-A001

February 9, 2018

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

On November 3, 2017, 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 appear in two documents: (1) the "[FATF Public Statement](#)," which includes jurisdictions that are subject to the FATF's call for countermeasures 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 includes jurisdictions identified by the FATF as having strategic AML/CFT deficiencies.² On November 3, 2017, 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: [Bosnia and Herzegovina](#), [Ethiopia](#), [Iraq](#), [Syria](#), [Vanuatu](#), and [Yemen](#)
- Added to list: [Sri Lanka](#), [Trinidad and Tobago](#), [Tunisia](#),
- Removed from list: [Uganda](#)

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 – www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/moreabouttheinternationalco-operationreviewgroupicrg.html.
3. See 31 U.S.C. § 5318(h) and (i).

I. Jurisdictions that are subject to the FATF’s call for countermeasures 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) consider the risk arising from each jurisdiction due to a lack of sufficient progress in addressing AML/CFT deficiencies.

Please click on each jurisdiction for additional information.

A. Countermeasures:

[Democratic People’s Republic of Korea \(DPRK\)](#)

B. Enhanced Due Diligence:

[Iran](#)

Summary of Changes to this List

- [DPRK](#): No changes.

The FATF remains concerned with the threat posed by illicit activities related to the proliferation of weapons of mass destruction (WMDs) and its financing emanating from the DPRK. Further, the FATF remains concerned with 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. In addition to enhanced scrutiny, the FATF further calls on its members and urges all jurisdictions to apply effective countermeasures, and targeted financial sanctions in accordance with applicable United Nations Security Council Resolutions (UNSCRs), to protect their financial sectors from money laundering, financing of terrorism, and WMD proliferation financing 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 UNSCRs.

See the full FATF statements on DPRK: <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/statement-dprk-nov-2017.html> and <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-november-2017.html>

- [Iran](#): No changes.

See the full FATF statements on Iran: <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-november-2017.html> and <http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-november-2017.html>

Review of Guidance Regarding 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 continues to reflect the high risk of proliferation finance attributable to the DPRK, consistent with UNSCRs 2397, 2375, 2371, 2270, and 2321. In particular, the FATF reaffirmed its call that jurisdictions terminate correspondent relationships with DPRK banks, where required by relevant UNSCRs. Financial institutions should be acutely aware of the financial provisions and prohibitions contained in the UNSCRs against the DPRK.⁴

In addition to UN sanctions, Treasury's Office of Foreign Assets Control (OFAC) maintains a robust sanctions program on North Korea through the North Korea Sanctions Regulations and Executive Orders (E.O.) 13382, 13466, 13551, 13570, 13687, 13722, and 13810.⁵ Collectively, these sanctions prohibit U.S. persons, including U.S. financial institutions, from engaging in nearly all transactions involving the DPRK.⁶ These sanctions are a direct response to North Korea's ongoing development of weapons of mass destruction (WMD) and their means of delivery in continued violation of the UNSCRs.

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with [E.O. 13810](#) (September 2017).⁷ Section 4 of E.O. 13810 allows OFAC to impose measures on foreign financial institutions that, on or after the date of the E.O., knowingly conduct or facilitate any significant transaction on behalf of a North Korea-related blocked person or knowingly conduct or facilitate any significant transaction in connection with trade with North Korea. The sanctions imposed since E.O. 13810 was issued have included actions against companies and individuals involved in shipping and transportation (including specific vessels), trading companies, financial representation, and banking.

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 <http://www.un.org/en/sc/documents/resolutions/> for more information.

5. See <https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx>.

6. Further information about these sanctions is available on [OFAC's Resource Center for DPRK Sanctions](#) and the [OFAC Recent Actions web page](#). OFAC most recently took new sanctions action related to DPRK, pursuant to Executive Orders 13687 and 13810 on [January 24, 2018](#). OFAC previously took sanctions actions related to DPRK on [December 26, 2017](#), pursuant to Executive Order 13687; on [November 21, 2017](#), pursuant to Executive Orders 13810 and 13722; on [October 26, 2017](#), pursuant to Executive Order 13687 and 13722; on [September 26, 2017](#), pursuant to Executive Order 13810; and on [August 22, 2017](#), pursuant to Executive Orders 13382 and 13722. OFAC took other DPRK-related sanctions pursuant to one or more of these same authorities on [June 29, 2017](#), [June 1, 2017](#), [March 31, 2017](#), [December 2, 2016](#), and [September 26, 2016](#). On November 20, 2017, the United States designated DPRK a state sponsor of terrorism, see <https://www.state.gov/j/ct/list/c14151.htm>.

7. See <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20170921.aspx> and <https://www.treasury.gov/press-center/press-releases/Pages/sm0162.aspx>.

Other Treasury actions underscore the serious risks that any financial activity involving the DPRK may facilitate WMD and ballistic missile activities. On November 4, 2016, Treasury issued a final rule, effective December 9, 2016, imposing the fifth special measure against the DPRK, consistent with the associated notice of finding that the DPRK is a jurisdiction of “primary money laundering concern” under Section 311 of the USA PATRIOT Act.⁸ The finding and rule stressed that the North Korean government continues to use state-controlled financial institutions and front companies to surreptitiously conduct illicit international financial transactions, some of which support the proliferation of weapons of mass destruction and the development of ballistic missiles. The final rule prohibits covered financial institutions from opening or maintaining in the United States correspondent accounts for, or 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, Treasury issued a final rule, effective December 8, 2017, under Section 311 of the USA PATRIOT Act that severs Bank of Dandong, a Chinese bank that acts as a conduit for illicit North Korean financial activity, from the U.S. financial system. The final action stressed that the Bank of Dandong acts as a conduit for North Korea to access the U.S. and international financial systems, including by facilitating millions of dollars of transactions for companies involved in North Korea’s WMD and ballistic missile programs. Bank of Dandong also facilitates 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.⁹

The Financial Crimes Enforcement Network (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 United Nations (UN) sanctions, launder funds, and finance the North Korean regime’s weapons programs.¹⁰

8. See <https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx> and <https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf> [81 FR 78715 (November 9, 2016)]. FinCEN issued the finding and notice of proposed rulemaking (NPRM) on June 1, 2016 [81 FR 35441 (June 2, 2016) and 81 FR 35665 (June 3, 2016)], respectively; see [https://www.fincen.gov/sites/default/files/shared/2016-13038\(DPRK_Finding\).pdf](https://www.fincen.gov/sites/default/files/shared/2016-13038(DPRK_Finding).pdf) and [https://www.fincen.gov/sites/default/files/shared/2016-13037\(DPRK_NPRM\).pdf](https://www.fincen.gov/sites/default/files/shared/2016-13037(DPRK_NPRM).pdf).

9. See <https://www.treasury.gov/press-center/press-releases/Pages/sm0205.aspx>, <https://www.treasury.gov/press-center/press-releases/Pages/jl0603.aspx>, and https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-02/Bank%20of%20Dandong%20311%20Final%20Rule.pdf [31 CFR Part 1010].

10. See FinCEN Advisories pertaining to the [DPRK: FIN-2017-A008](#) (November 2, 2017), [FIN-2013-A005](#), [FIN-2009-A002](#), and [FinCEN Advisory – Issue 40](#).

Iran

The FATF's decision to continue the suspension of its call for countermeasures against Iran does not remove or alter any obligations U.S. financial institutions may have with respect to Iran under U.S. law and regulation. The FATF reiterated the significant terrorist financing risk emanating from Iran and the threat this poses to the international financial system. U.S. financial institutions are still subject to a broad range of restrictions and prohibitions on engaging in transactions with or involving Iran due to a number of illicit finance risks, including money laundering, terrorist financing, and the financing of Iran's ballistic missile program. U.S. financial institutions must continue to comply with existing U.S. sanctions on Iran. These sanctions include general prohibitions on engaging in transactions or dealings with or involving Iran, the Government of Iran, Iranian financial institutions, and certain designated persons. Designated persons include individuals and entities appearing on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List), including those linked to Iran's ballistic missile program and support to terrorism. Since February 2017, OFAC has issued eleven new rounds of designations relating to Iran.¹¹ Recent designations have targeted, among other things, serious human rights abuses by the Government of Iran, grave human rights abuses by the Government of Iran via information technology; censorship or other activities that prohibit, limit, or penalize the exercise of freedom of expression or assembly by citizens of Iran, or that limit access to print or broadcast media; and ballistic missile development.

Treasury has consistently underscored the risks of conducting business associated with Iran. On November 28, 2011, Treasury issued an NPRM to impose a special measure against Iran based on its finding that Iran is a jurisdiction of "primary money laundering concern" under Section 311 of the USA PATRIOT Act.¹² Financial institutions also should be familiar with the financial provisions and prohibitions contained in UNSCR 2231 related to Iran.¹³

-
11. Information about these sanctions is publicly available on OFAC's [Iran Sanctions web page](#) and the [OFAC Recent Actions web page](#). On [January 12, 2018](#), [January 4, 2018](#), [November 20, 2017](#), [October 31, 2017](#), and [October 13, 2017](#), OFAC issued new Iran-related designations. 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](#).
 12. See 76 FR 72756 (Nov. 25, 2011), [Finding that the Islamic Republic of Iran is a Jurisdiction of Primary Money Laundering Concern](#). FinCEN continues to assess the appropriateness of finalizing the rule.
 13. See UNSCR 2231 (July 2015) relating to implementation of the Joint Comprehensive Plan of Action of July 14, 2015 (JCPOA) provides that, when the International Atomic Energy Agency (IAEA) verified that Iran completed certain nuclear commitments under the JCPOA: (1) prior Iran-related UNSCRs (including UNSCRs 1929 (June 2010), 1803 (March 2008), 1747 (March 2007), and 1737 (December 2006)) would be terminated and (2) states would simultaneously comply with certain provisions of Annex B to UNSCR 2231, including paragraph 6 relating to financial provisions and restrictions for listed individuals and entities. On January 16, 2016, the IAEA issued its report verifying that Iran had completed certain nuclear commitments under the JCPOA; as a result, UNSCRs 1929, 1803, 1747, and 1737 were terminated, and the measures described in Annex B of UNSCR 2231 came into effect. See also <http://www.un.org/en/sc/2231/> for more information.

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

FinCEN advises U.S. financial institutions to apply enhanced due diligence when maintaining correspondent accounts for foreign banks operating under a banking license issued by a designated country.¹⁴ Financial institutions must also 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.

As required by the regulations implementing the Bank Secrecy Act, covered financial institutions should 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.¹⁵

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](#)".

14. 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 foreign banks). The obligations under Section 312 of the USA PATRIOT Act are consistent with FATF's statements on the DPRK and Iran.

15. See 31 CFR § 1010.610(b): Enhanced Due Diligence for correspondent accounts established, maintained, administered or managed in the United States for foreign banks.

Please click on each jurisdiction for additional information.

[Bosnia and Herzegovina](#), [Ethiopia](#), [Iraq](#), [Sri Lanka](#), [Syria](#), [Trinidad and Tobago](#), [Tunisia](#), [Vanuatu](#), and [Yemen](#).

Summary of changes to this list

Countries Removed from the List

- [Uganda](#) is no longer subject to the FATF’s on-going global AML/CFT compliance process. The FATF has found that Uganda has made significant technical progress in improving its AML/CFT regime and has established the legal and regulatory framework to meet the commitments in its action plan. Uganda will work with the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) as it continues to address the full range of AML/CFT issues identified in its mutual evaluation report.

Countries Added to the List

- [Sri Lanka](#) has been added to this list due to the lack of effective implementation of its AML/CFT framework. Sri Lanka has made a high-level political commitment to work with the FATF and the Asia/Pacific Group on Money Laundering (APG) to strengthen the effectiveness of its AML/CFT regime and address any related technical deficiencies.
- [Trinidad and Tobago](#) has been added to this list due to the lack of effective implementation of its AML/CFT framework. Trinidad and Tobago made a high-level political commitment to work with the FATF and the Caribbean Financial Action Task Force (CFATF) to strengthen the effectiveness of its AML/CFT regime and address any related technical deficiencies.
- [Tunisia](#) has been added to this list due to the lack of effective implementation of its AML/CFT framework. Tunisia has made a high-level political commitment to work with the FATF and The Middle East and North Africa Financial Action Task Force (MENAFATF) to strengthen the effectiveness of its AML/CFT regime and 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 countries identified under this section ([Bosnia and Herzegovina](#), [Ethiopia](#), [Iraq](#), [Sri Lanka](#), [Syria](#), [Trinidad and Tobago](#), [Tunisia](#), [Vanuatu](#), and [Yemen](#)).¹⁶ With respect to these jurisdictions, U.S. financial institutions are reminded of their obligations to comply with

16. 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](#).

the general due diligence obligations under 31 CFR § 1010.610(a) in addition to their general obligations under 31 U.S.C. § 5318(h) and its implementing regulations.¹⁷ As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for foreign financial institutions, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States. 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.¹⁸

Review of General Guidance

AML Program Risk Assessment: For the jurisdiction that was removed from the FATF listing and monitoring process ([Uganda](#)), 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 § 1010.210.¹⁹

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.²⁰

17. *See, generally*, 31 CFR § 1010.210: Anti-money laundering programs. Specific AML Program obligations are proscribed 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).

18. *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.

19. *Ibid.*

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

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 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.

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.