

FIN-2018-A002

April 27, 2018

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

On February 23, 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 appear in two documents: (1) the "[FATF Public Statement](#)," which includes 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 includes jurisdictions identified by the FATF as having strategic AML/CFT deficiencies.² On February 23, 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](#), [Iraq](#), [Sri Lanka](#), [Syria](#), [Trinidad and Tobago](#), [Tunisia](#), [Vanuatu](#), and [Yemen](#)
- Added to list: [Serbia](#)
- Removed from list: [Bosnia and Herzegovina](#)

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) 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 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 UN Security Council Resolutions (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 comprehensive prohibitions contained in the UNSCRs imposing sanctions on the DPRK and the risks to institutions.⁴

Among other prohibitions and restrictions, UNSCR [2321](#), adopted in 2016, states that a member state shall expel individuals whom the member state determines are acting on behalf of or at the direction of a bank or financial institution of the DPRK. UNSCR 2321 also expressed concern that individuals from the DPRK are sent abroad to earn hard currency to fund the DPRK's nuclear and ballistic missile programs and reiterated the UN Security Council's concern that the DPRK may use bulk cash to evade 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 <http://www.un.org/en/sc/documents/resolutions/> for more information.

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, 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 Collectively, these authorities 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 the DPRK’s ongoing development of weapons of mass destruction (WMD) and their means of delivery; the launching of intercontinental ballistic missiles; nuclear tests; human rights abuses and censorship; destructive, coercive cyber-related actions; and involvement in money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking, in continued violation of the UNSCRs.⁷

U.S. financial institutions should be particularly aware of the extensive nature of the sanctions associated with [E.O. 13810](#) (September 2017).⁸ The E.O. provides the Secretary of the Treasury, in consultation with the Secretary of State, additional tools to disrupt North Korea’s ability to fund its weapons of mass destruction (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 linked to North Korea that come within the United States or possession of a United States person; and (4) provides authority to impose sanctions on a foreign financial institution that knowingly conducted or facilitated on or after the date of the order (i) any significant transaction on behalf of certain blocked persons or (ii) any significant transaction in connection with trade with North Korea. The sanctions applicable to foreign financial institutions can be restrictions on correspondent or payable-through accounts or full blocking sanctions.⁹

-
5. See <https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx>, 22 U.S.C. § 9201 et seq. , and [Public Law 115-44](#)
 6. 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 new sanctions actions related to the DPRK pursuant to Executive Orders [13810](#) and [13722](#) on [February 23, 2018](#). OFAC also issued a related [North Korea Sanctions Advisory](#) on sanctions risks related to North Korea’s shipping practices. OFAC issued DPRK-related sanctions pursuant to Executive Orders [13687](#), [13722](#), and [13810](#) on [January 24, 2017](#). OFAC imposed DPRK-related sanctions actions pursuant to Executive Orders [13810](#) and [13722](#) on [November 21, 2017](#). OFAC took 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, see <https://www.state.gov/j/ct/list/c14151.htm>.
 7. See Executive Orders [13810](#) ([September 20, 2017](#)), [13687](#) ([January 2, 2015](#)), and [13551](#) ([August 30, 2010](#)).
 8. 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>.
 9. See https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#525

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.¹⁰ Additionally, on February 23, 2018, with the U.S. Department of State and the U.S. Coast Guard, OFAC issued an advisory to alert persons globally of North Korea’s deceptive shipping practices to evade U.S. and UN sanctions.¹¹

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, 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.¹² 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.¹³ 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 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

10. See Executive Order 13810 ([September 20, 2017](#)).

11. See <https://home.treasury.gov/news/press-releases/sm0297>

12. 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); 31 CFR § 1010.659]. 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), 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).

13. See <https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf> [31 CFR § 1010].

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.¹⁴

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.¹⁵

Iran

The FATF kept Iran on its Public Statement and called upon its members and all jurisdictions to apply enhanced due diligence measures proportionate to the risks arising from Iran. Furthermore, FATF highlighted Iran's failure to address the majority of its AML/CFT action plan requirements and, for the first time, provided a comprehensive list of Iran's major deficiencies in its AML/CFT regime.

The FATF 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 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 offense; and (9) ensuring adequate legislation and procedures to provide for confiscation of property of corresponding value."¹⁶

The FATF also reiterated the significant terrorist financing risk emanating from Iran and the threat this poses to the international financial system. The FATF will assess Iran's actions and consider further steps at its next meeting, June 24-29, 2018. The FATF's decision to continue the suspension of its call for countermeasures against Iran while keeping Iran on the Public Statement does not remove or alter any obligations U.S. financial institutions may have with respect to Iran under U.S. law and regulation.

U.S. financial institutions are 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

14. 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 - [82 FR 51758 (November 8, 2017); 31 CFR § 1010.660].

15. See FinCEN Advisory [FIN-2017-A008 \(November 2, 2017\)](#). In addition, FinCEN has three other advisories relating to the DPRK: [FIN-2013-A005](#), [FIN-2009-A002](#) and [FinCEN Advisory – Issue 40](#).

16. See [http://www.fatf-gafi.org/fr/publications/jurisdictionshautrisqueetnoncooperatives/documents/public-statement-february-2018.html?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/fr/publications/jurisdictionshautrisqueetnoncooperatives/documents/public-statement-february-2018.html?hf=10&b=0&s=desc(fatf_releasedate)).

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 11 new rounds of designations relating to Iran.¹⁷ Pursuant to Executive Orders 13224, 13382, 13553, 13581, 13606, 13628, and 13694, 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; support for terrorism; weapons proliferators; and ballistic missile development. OFAC designations have also targeted individuals and entities linked to the Islamic Revolutionary Guard Corps (IRGC) and IRGC-Qods Force (IRGC-QF) specifically.¹⁸ The IRGC and the IRGC-Qods Force engage in seemingly legitimate activities that provide cover for intelligence operations and support terrorist groups such as Hizballah, Hamas, and the Taliban. The IRGC has an extensive presence in Iran’s economy, which is obscured by a lack of transparency given significant deficiencies in its AML/CFT regime.

Financial institutions should be familiar with the financial provisions and prohibitions contained in UNSCR 2231 related to Iran.¹⁹ Treasury has consistently underscored the risks of conducting business associated with Iran. On November 28, 2011, FinCEN issued an NPRM proposing the imposition of 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.²⁰

17. Information about these sanctions is publicly available on OFAC’s [Iran Sanctions web page](#) and the [OFAC Recent Actions web page](#). On [March 23, 2018](#), [January 12, 2018](#), [January 4, 2018](#), [November 20, 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](#). The [October 31, 2017](#) document was an update to the SDN List. OFAC did not designate new entities or persons.

18. See OFAC’s [Iran Sanctions web page](#) and the [OFAC Recent Actions web page](#) and designations made on [January 12, 2018](#), [November 20, 2017](#), [October 13, 2017](#), [September 14, 2017](#), [July 18, 2017](#), and [February 3, 2017](#).

19. See UNSCR 2231 (July 2015), relating to implementation of the Joint Comprehensive Plan of Action of July 14, 2015 (JCPOA), which 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.

20. 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.

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

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 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.²¹ 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, as amended by the U.S. PATRIOT 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.²²

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](#)".

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

22. *Id.*

Please click on each jurisdiction for additional information.

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

Summary of changes to this list

Countries Removed from the List

- [Bosnia and Herzegovina](#) is no longer subject to the FATF’s on-going global AML/CFT compliance process. The FATF has found that Bosnia and Herzegovina 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. Bosnia and Herzegovina will continue to work with MONEYVAL to improve its AML/CFT framework.

Countries Added to the List

- [Serbia](#) has been added to this list due to the lack of effective implementation of its AML/CFT framework. Serbia has made a high-level political commitment to work with the FATF and MONEYVAL to strengthen the effectiveness of its AML/CFT regime and address related technical deficiencies. The FATF highlighted the specific deficiencies in Serbia’s AML/CFT regime.

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](#), [Iraq](#), [Serbia](#), [Sri Lanka](#), [Syria](#), [Trinidad and Tobago](#), [Tunisia](#), [Vanuatu](#), and [Yemen](#)).²³ With respect to these jurisdictions, U.S. financial institutions are reminded of their obligations to comply with the general due diligence obligations for foreign financial institutions under 31 CFR § 1010.610(a) in addition to their general obligations under 31 U.S.C. § 5318(h) and its implementing regulations.²⁴ 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,

23. 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](#).

24. 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).

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.²⁵

Review of General Guidance

AML Program Risk Assessment: For the jurisdiction that was removed from the FATF listing and monitoring process ([Bosnia and Herzegovina](#)), 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 1010.210.²⁶

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.²⁷

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:**

“FEBRUARY 2018 FATF STATEMENTS”

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

25. 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.

26. *Supra* note 17.

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

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.²⁸

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.

28. For example case studies, see SAR Activity Review, Issue 19, beginning on page 25, and [Law Enforcement Case Examples](#).