UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

ADVISORY

FIN-2017-A004 **September 6, 2017**

Advisory on Political Corruption Risks in South Sudan

Certain South Sudanese senior political figures may seek to abuse the financial system to move and hide corruption proceeds.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operations Officers*
- *Chief Risk Officers*
- *Chief Compliance Officers*
- *Legal departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to alert U.S. financial institutions about the possibility that certain South Sudanese senior political figures may try to use the U.S. financial system to move or hide proceeds of public corruption. This advisory reminds financial institutions of their due diligence and suspicious activity report (SAR) filing obligations related to such senior foreign political figures.[1] It also highlights persons who have been subject to sanctions because of their actions threatening the peace, security, or stability of South Sudan. High-level political corruption can damage a nation's economic growth and stability as it can interfere with the international community's efforts to support and promote economic development, discourage foreign private investment, and foster a climate where financial crime and other forms of lawlessness can thrive.

Situation in South Sudan

The U.S. Department of State has been publicly documenting the unfolding situation in South Sudan.[2] As noted, in 2011, after a bloody and protracted conflict, the Republic of South Sudan gained formal independence from the Republic of Sudan. In 2013, a new political conflict began

1. "The term 'senior foreign political figure' means a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not); a senior official of a major foreign political party; or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity that has been formed by, or for the benefit of, any such individual; an immediate family members of any such individual; and a person who is widely and publicly known (or is actually known by the relevant covered financial institution) to be a close associate of such individual. For the purposes of this definition, 'senior official or executive' means an individual with substantial authority over policy, operations, or the use of government-owned resources and 'immediate family member' means spouses, parents, siblings, children and a spouse's parents and siblings." 31 CFR § 1010.605(p). See also generally 31 CFR § 1010.620 and 31 CFR § 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

2. For more details on these events and their significant adverse impact on South Sudanese society, see U.S. Department of State, U.S. Relations with South Sudan and U.S. Embassy in South Sudan; U.S. Department of State, *Country Reports for Human Rights Practices* (2016), "South Sudan". See also Central Intelligence Agency, *The World Fact Book*, "South Sudan".

within the ruling party of the nascent South Sudanese nation, growing into a broader conflict. An estimated 1.9 million South Sudanese have fled to neighboring countries, with another two million displaced internally, including more than 200,000 civilians who have sought refuge in UN-protected camps within South Sudan. The warring parties have failed to adhere to an agreed ceasefire, leaving the civilian population suffering through widespread violence and atrocities, human rights abuses, recruitment and use of child soldiers, attacks on peacekeepers, and obstruction of humanitarian operations. The ongoing conflict also has resulted in widespread food insecurity.

South Sudanese Political Corruption

During this time of internal conflict and devastation, certain South Sudanese senior political officials, representing both the government and the opposition, have engaged in and profited from corrupt practices.[3] According to the U.S. Department of State, various forms of endemic corruption in South Sudan have increased since the beginning of the South Sudanese Civil War in December 2013. For example:

- ***Abuse of position and use of shell companies***: Government officials have regularly abused their positions to enrich themselves illegally under the guise of conducting government business. South Sudanese government corruption is often conducted through the use of shell companies belonging to the relatives of government officials.
- ***Abuse of government contracting, particularly involving natural resources***: Government officials misappropriate public funds outside the parliament-approved budget to supplement limited government salaries and to enrich themselves. Corrupt officials steer government contracts to businesses—particularly in the natural resource (oil and gas) sector—in which they, their family members, or close associates have some level of beneficial ownership and control.
- ***Use of international financial system and real estate***: The funds accumulated through the proceeds of South Sudanese corruption are moved to accounts outside of South Sudan. Once the funds are held in accounts in other countries, they are used to purchase real estate (among other things) in third countries.
- ***Abuse of military procurement***: South Sudan's military spending is the highest in the region. Public reporting indicates that senior military officials in South Sudan have also engaged in corrupt practices similar to their political counterparts to enrich themselves, their families and associates. Corruption has been particularly egregious in the procurement of military matériel and services, which account for nearly half of South Sudan's annual budget.

3. See U.S. Department of State, *Country Reports for Human Rights Practices* (2016), "South Sudan," Section 4, "Corruption and Lack of Transparency in Government" and U.S. Department of State, *Investment Climate Statements* (2016), "South Sudan," July 5, 2016.

- ***Abuse of military payrolls***: Corruption in the military payroll system also is rampant: generals appear to routinely siphon off civilian budgets for their personal benefit or of their organizations, as well as to procure arms and supplies that have directly threatened the peace, stability, and security of South Sudan. Military commanders have even reportedly stolen soldiers' salaries. Another example is the proliferation of "ghost soldiers"—fictitious soldiers who only exist on payroll documents—has been identified by academics and journalists as one of the primary means by which funds are diverted to senior military officials.

Designated South Sudanese Persons

To further assist U.S. financial institutions' efforts to protect the U.S. financial system from laundering the proceeds of corruption, FinCEN is providing information on South Sudan sanctions designations by the United States and the United Nations. Including the September 6, 2017 designations, the United States has now sanctioned nine South Sudanese persons and three companies.[4] The United Nations has sanctioned six of those same persons. As warranted, the United States may issue further designations related to South Sudan.

OFAC Designated Individuals and Entities

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has designated certain persons in South Sudan pursuant to Executive Order (E.O.) 13664 ("Blocking Property of Certain Persons with Respect to South Sudan," issued on April 3, 2014, placing them on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List).[5]

The OFAC sanctions broadly prohibit U.S. persons, including U.S. financial institutions, from engaging in transactions involving designated individuals and entities, including but not limited to the making or receipt of any contribution or provision of funds, goods, or services by, to, for, or from such persons without a general or specific OFAC license or applicable exemption. For each designated person, all property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any U.S. person, are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in.

4. *See* https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/OFAC-Recent-Actions.aspx.
5. OFAC has designated these persons pursuant to E.O. 13664, which authorizes the imposition of targeted sanctions against specifically identified individuals and entities determined to be engaged in certain activities in South Sudan, including threatening the peace, security, or stability of South Sudan; extending or expanding the conflict in South Sudan; engaging in widespread violence and atrocities, human rights abuses, recruitment and use of child soldiers, attacks on peacekeepers, or obstruction of humanitarian operations in South Sudan; or being a leader of a group involved in the aforementioned activities in South Sudan. See the OFAC press center for more information on these designations.

United Nations Sanctioned Individuals

United Nations Security Council Resolution (UNSCR) 2206, adopted on March 3, 2015, established a global regime of targeted sanctions on individuals and entities to support the search for an inclusive and sustainable peace in South Sudan. The Security Council has renewed UN sanctions with respect to South Sudan annually, most recently in UNSCR 2353 (May 24, 2017). The UN sanctions are managed by a sanctions committee (Security Council Committee on South Sudan, or "Committee").[6] The UN sanctions place a travel ban and an asset freeze on individuals and entities designated by the Committee as responsible for or complicit in, or having engaged in, directly or indirectly, actions or policies that threaten the peace, security, or stability of South Sudan.[7] Member states of the United Nations are required to administer and enforce domestic sanctions in compliance with UN sanctions regimes.

On July 1, 2015, the Committee designated individuals pursuant to UNSCR 2206, all of whom are also designated by OFAC.[8]

AML Guidance and Regulatory Obligations for U.S. Financial Institutions regarding Senior Foreign Political Figures and Suspicious Activity Reporting

The OFAC and UN designations increase the likelihood that other, non-designated South Sudanese senior political figures and opposition leaders may seek to protect their assets, including those that are likely to be associated with political corruption, to avoid potential future blocking actions.

Consistent with existing regulatory obligations, financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with South Sudanese corruption. Such reasonable steps should not, however, put

6. *See* UN Secretary General Ban Ki-Moon Statement SG/SM/16562-AFR/308, March 3, 2015 and United Nations Security Council Resolution 2206 (March 2015).
7. See Letter from the Panel of Experts on South Sudan established pursuant to Security Council resolution 2206 addressed to the President of the Security Council (January 2016).
8. See The List established and maintained pursuant to UNSCR 2206.
9. 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.

into question a financial institution's ability to maintain or 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.[9]

Due diligence obligations

FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting their due diligence obligations that may apply to activity involving certain South Sudanese persons. To best meet these obligations, financial institutions should generally be aware of public reports of high-level corruption associated with certain senior foreign political figures, family members, associates, or associated legal entities or arrangements. Financial institutions should assess the risk for laundering of the proceeds of public corruption associated with specific particular customers and transactions.

Enhanced due diligence obligations for private bank accounts

Under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)), U.S. financial institutions have regulatory obligations to apply enhanced scrutiny to private banking accounts held by, or on behalf of, senior foreign political figures and to monitor transactions that could potentially represent misappropriated or diverted state assets, the proceeds of bribery or other illegal payments, or other public corruption proceeds.[10]

These implementing regulations require a written due diligence program for private banking accounts held for non-U.S. persons designed to detect and report any known or suspected money laundering or other suspicious activity.[11] In instances where senior foreign political figures maintain private banking accounts at a covered institution, those financial institutions are required to apply enhanced scrutiny of such accounts to detect and report transactions that may involve the proceeds of foreign corruption.[12]

General obligations for correspondent account due diligence and anti-money laundering programs

U.S. financial institutions also are reminded to comply with their general due diligence obligations under 31 CFR § 1010.610(a), in addition to their general AML Program obligations under 31 U.S.C. § 5318(h) and its implementing regulations.[13] As required under 31 CFR § 1010.610(a),

10. *See generally* 31 CFR § 1010.620 and 1010.210 as further proscribed in 31 CFR § 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1029.210, and 1030.210

11. *See* 31 CFR § 1010.620(a-b). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).

12. 31 CFR § 1010.620(c).

13. 31 CFR § 1010.210: Anti-money laundering programs.

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.

Suspicious Activity Reporting

A financial institution may be required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the Bank Secrecy Act (BSA); lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[14]

Additional SAR reporting guidance on Senior Foreign Political Figures

In April 2008, FinCEN issued Guidance to assist financial institutions with reporting suspicious activity regarding proceeds of foreign corruption.[15] A related FinCEN SAR Activity Review, which focused on foreign political corruption, also discusses indicators of transactions that may be related to proceeds of foreign corruption.[16] Financial institutions may find this Guidance and the SAR Activity Review useful in assisting with suspicious activity monitoring and due diligence requirements related to senior foreign political figures.

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 **select SAR field 35(l) (Suspected Public/Private Corruption (Foreign)) and reference this advisory by including the key term:**

"SOUTH SUDAN"

in the SAR narrative and in SAR field 35(z) (Other Suspicious Activity-Other) to indicate a connection between the suspicious activity being reported and the persons and activities highlighted in this advisory.

14. *See generally* 31 CFR § 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
15. *See* FinCEN Guidance FIN-2008-G005: "Guidance to Financial Institutions on Filing Suspicious Activity Reports Regarding the Proceeds of Foreign Corruption," (April 2008).
16. *See* Bank Secrecy Act Advisory Group "Focus: Foreign Political Corruption," SAR Activity Review, Issue 19, May 2011, particularly pages 29-69.

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying money laundering and other financial crimes associated with foreign and domestic political corruption. 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.[17]

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.

17. *See* example case studies at the above SAR Activity Review, Issue 19, beginning on page 25 and Law Enforcement Case Examples.