UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

December 1, 2015

Non-Public Advisory

Secure Information Sharing System Advisory

Advisory to Financial Institutions on the Financing of Foreign Terrorist Fighters

This advisory should be shared with:

- *AML/BSA management**
- *AML data analytics teams**
- *AML intelligence units**
- *AML analysts/investigators**
- *IT Security departments**

*** Contact FinCEN before sharing this information outside of your organization**

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to provide financial institutions with information on identifying and reporting transactions possibly associated with Foreign Terrorist Fighters (FTFs) who support the Islamic State of Iraq and the Levant (ISIL), al-Qa'ida, and their affiliates in Iraq and the Levant region.[1] Financial institutions may use this information to enhance their Anti-Money Laundering (AML) risk-based strategies and monitoring systems. This advisory is not intended to call into question financial institutions' maintenance of normal relationships with other financial institutions, or to be used as basis for engaging in wholesale or indiscriminate de-risking practices.[2]

Foreign Terrorist Fighters (FTFs): Individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict.

Since the issuance of FinCEN's non-public advisory on ISIL financing in May 2015, ISIL has expanded its presence and its financial network may have branched out. These developments may facilitate ISIL's recruitment of foreign terrorist fighters who join its militant forces or carry out terrorist attacks in different parts of the world. The United Nations estimates more than 25,000 men and women in over 100 countries have left their homes to become foreign terrorist fighters in Iraq, Libya, and Syria.[3]

1. For the purposes of this advisory, the Levant region consists of Israel, Jordan, Lebanon, the Palestinian Territories, and Syria.
2. De-risking refers to the practice of discontinuing or restricting business relationships with categories of clients to avoid, rather than manage, risk in line with a risk-based approach.
3. Secretary-General's remarks to Security Council meeting on Threats to International Peace and Security Caused by Terrorist Acts (Foreign Terrorist Fighters) (May, 2015), available at www.un.org/sg/statements/index.asp?nid=8689.

Activity Possibly Associated With FTFs

Once recruited, FTFs seek to travel to areas where ISIL, al-Qa'ida, and their affiliates operate, such as Iraq and the Levant region. Accordingly, financial activity of FTFs may reflect transactions related to their travel preparations and arrangements, departure, in-transit period, and arrival and presence in the conflict zone.

FTFs may use diverse methods to disguise their finances or intentions. When determining whether transactions may be related to the financing of an FTF, financial institutions should consider multiple factors in addition to the red flags identified in the next section below, including:

- Deviation from a customer's normal activity;
- Source of funds;
- Available information on the purpose of transactions;
- Publicly available information; and
- Whether a customer exhibits several of the red flags mentioned in this advisory and/or in FinCEN's May 2015 non-public advisory on ISIL financing.[4]

With respect to publicly available information, for instance, ISIL and other terrorist organizations are known to be active on social media sites. Financial institutions may find available social media information helpful in evaluating potential suspicious activity and in identifying risks connected to the red flags provided in this and other advisories. Similarly, the location from which a customer logs into a financial institution's online services platform may also be considered when determining whether a transaction is suspicious (see next section).

Red Flags

In applying the red flags below, financial institutions are advised that no single transactional red flag is a clear indicator of terrorist activity. Financial institutions should consider additional factors, such as a customer's overall financial activity and whether he or she exhibits multiple red flags, before determining a possible association to terrorist financing and FTFs. Financial institutions should also refer to the red flags and other information provided in this and the May 2015 non-public advisory to formulate a more comprehensive assessment of potential suspicious activity.

Depending on their products and services offered, financial institutions may be able to observe one or more of the following red flags. Some of these red flags may be observed during general transactional screening, while others may be more readily identified during in-depth case reviews.

Activities Prior to Departure: Prospective FTFs make typical financial and logistical preparations prior to traveling. Transactions associated with FTFs may include:

- Purchasing goods at camping or survival stores;
- Purchasing first-person shooter games or engaging in combat training-type activities;

4. Available at FinCEN's Secured Information Sharing System (https://www.fincen.gov/314a/).

Red Flags
(continued)

- Purchase of airfare and payment of travel related fees (e.g., visa fees) involving countries in Europe or countries near or adjacent to ISIL-controlled areas—including Cyprus, Egypt, Greece, Jordan, Lebanon, and Turkey;
- Establishing lines of credit and taking out personal loans where no loan repayments are made;
- Liquidating personal assets, including retirement accounts/plans, and obtaining life insurance policies;
- Receiving funds from or sending funds to seemingly unrelated individuals who are located near cities with a reported ISIL/al-Qa'ida-presence, where the transactions do not appear to have a lawful business purpose. These seemingly unrelated individuals may share common or similar addresses, telephone numbers, or other identifying information; and
- Customers with minimal activity before ISIL's expanded operations (early 2014) now showing inflows from unknown origins followed by fund transfers to beneficiaries (or ATM withdrawals) in Iraq, northeastern Lebanon, Libya, southern Turkey, or Syria.

Activities While in Transit to or in Conflict Zone: To reach Iraq or the Levant region, FTFs may purchase airline tickets to countries in Europe or to countries near or adjacent to ISIL/al-Qa'ida-controlled areas—including Cyprus, Egypt, Greece, Jordan, Lebanon, and Turkey—before continuing by land. In this regard, transactions, ATM withdrawals, or online logins may be observable at transit points along their route.

In addition, FTFs may use funds for provisions, training, or operating while in transit or in the conflict zone. This behavior may be characterized by suspicious activity originating in cities near ISIL/al-Qa'ida-controlled areas including unusual online logins, ATM withdrawals, or funds transfers.

- FTFs and ISIL associates may use a financial institution's online tools, or customer service phone lines, to remotely monitor transactions for the purpose of coordinating and facilitating the collection of funds or initiating additional transactions. For instance, transactions initiated within the United States may be followed by near-time online-logins from locations in Syria, Iraq, northeastern Lebanon, or the Turkish southern border region;
- Financial institutions may be able to determine if an online login is suspicious by ascertaining whether the involved IP address originates from a country different from that of the customer;
- In attempts to communicate with others and to avoid telecommunications or e-mails, FTFs may send small-amount fund transfers (e.g., $1), where payment instructions or transaction descriptions include suspicious short messages; and
- After exhibiting the above-mentioned behaviors/red flags and following a long period of inactivity, possible FTFs may start conducting transactions along transit points located between their country of origin and Iraq or the Levant region. This activity may indicate a possible FTF returning to his/her home country.

SAR Reporting and Guidance to U.S. Financial Institutions

Financial institutions wanting to report suspicious transactions that may relate to terrorism or terrorist financing 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 also immediately report any imminent threat to local/federal law enforcement officials.

Financial institutions reporting terrorist financing through Suspicious Activity Reports (SARs) are reminded to include all relevant information in the form, to mark SAR-checkbox 30(a) or 30(z) (Terrorist Financing), and to provide detailed information, including IP addresses, in the narrative section of the SAR. Financial institutions should also reference this Advisory in the narrative section when filing a SAR.

Additional Information

Additional questions or comments regarding the contents of this Advisory or with respect to instructions on its further dissemination should be addressed to FinCEN at (800) 767-2825 (Option 9), (703) 905-3591 (Option 9), or at FRC@fincen.gov.

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.