(BILLINGCODE: 4810-02)

**DEPARTMENT OF THE TREASURY**

**Financial Crimes Enforcement Network**

**Notice of Finding that FBME Bank Ltd., Formerly Known as Federal Bank of the Middle East, Ltd., is a Financial Institution of Primary Money Laundering Concern**

**AGENCY:** Financial Crimes Enforcement Network ("FinCEN"), Treasury.

**ACTION:** Notice of finding.

**SUMMARY:** This document provides notice that, pursuant to the authority contained in 31 U.S.C. 5318A, the Director of FinCEN found on July 15, 2014, that reasonable grounds exist for concluding that FBME Bank Ltd. ("FBME" or the "Bank"), formerly known as Federal Bank of the Middle East, Ltd., defined to include all of its branches, subsidiaries, and offices, is a financial institution operating outside of the United States of primary money laundering concern.

**DATES:** The finding referred to in this notice was effective as of July 15, 2014.

**FOR FURTHER INFORMATION CONTACT:** FinCEN, (800) 767-2825.

**SUPPLEMENTARY INFORMATION:**

## I. Statutory Provisions

On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA PATRIOT Act"), Public Law 107-56. Title III of the USA PATRIOT Act amends the anti-money laundering ("AML") provisions of the Bank Secrecy Act ("BSA"), codified at 12 U.S.C. 1829b, 12 U.S.C 1951-1959, and 31 U.S.C. 5311-5314, 5316-5332, to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Regulations implementing the BSA appear at 31 CFR Chapter X. The authority of the Secretary of

the Treasury (the "Secretary") to administer the BSA and its implementing regulations has been delegated to the Director of FinCEN.

Section 311 of the USA PATRIOT Act ("Section 311"), codified at 31 U.S.C. 5318A, grants the Director of FinCEN the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, financial institution, class of transaction, or type of account is of "primary money laundering concern," to require domestic financial institutions and financial agencies to take certain "special measures" to address the primary money laundering concern.

## II. History of FBME and Jurisdictions of Operation

FBME was established in 1982 in Cyprus as the Federal Bank of the Middle East, Ltd., a subsidiary of the private Lebanese bank, Federal Bank of Lebanon. Both FBME and the Federal Bank of Lebanon are owned by Ayoub-Farid M. Saab and Fadi M. Saab. In 1986, FBME changed its country of incorporation to the Cayman Islands, and its banking presence in Cyprus was re-registered as a branch of the Cayman Islands entity. In 2003, FBME left the Cayman Islands due to problems with capital adequacy regulations and re-established itself in Tanzania by acquiring Delphis Bank, a small Tanzanian financial institution with three bank branches. At the same time, FBME's Cypriot operations became a branch of FBME Tanzania Ltd. In 2005, FBME formally changed its name from Federal Bank of the Middle East, Ltd. to FBME Bank Ltd.

Since 2003, FBME has been headquartered in Tanzania. FBME headquarters is widely regarded as the largest bank in Tanzania based on its $2 billion asset size, but it has only four branches. While FBME is presently headquartered in Tanzania, FBME transacts over 90% of its global banking business and holds over 90% of its assets in its

Cyprus branch. FBME has always maintained a significant presence in Cyprus. FBME has stated, however, that it is not in direct competition with local retail banks in Cyprus for several reasons, including that it does not issue checks, has no retail counters, and its Cypriot customers are limited to mainly staff, contractors, and professionals providing services to FBME.

The Central Bank of Cyprus ("CBC"), which supervises and regulates all Cypriot banks, including branches of foreign financial institutions such as FBME, has found FBME's compliance with Cypriot banking laws and AML regulations deficient on at least two occasions. As evidenced by its failure to comply with the Cypriot AML law, FBME's weak AML controls and customer due diligence resulted in a fine by the CBC in 2008. In addition, in 2013, FBME took active steps to evade oversight by the Cypriot regulatory authorities. In November 2013, the CBC stated that FBME may be subject to sanctions and a fine of up to 240 million euro for alleged violations of capital controls.

## III. The Extent to Which FBME Has Been Used to Facilitate or Promote Money Laundering In or Through Cyprus and Tanzania

### 1. FBME Facilitates Money Laundering, Terrorist Financing, Transnational Organized Crime, Fraud Schemes, Sanctions Evasion, Weapons Proliferation, Corruption by Politically-Exposed Persons, and Other Financial Crimes.

FBME facilitated a substantial volume of money laundering through the Bank for many years. FBME is used by its customers to facilitate money laundering, terrorist financing, transnational organized crime, fraud, sanctions evasion, and other illicit activity internationally and through the U.S. financial system. FBME has systemic failures in its AML controls that attract high-risk shell companies, that is, companies formed for the sole purpose of holding property or funds and that do not engage in any

legitimate business activity. FBME performs a significant volume of transactions and activities that have little or no transparency and often no apparent legitimate business purpose.

Through relationships developed by FBME's management since at least 2006, as well its large shell company customer base, FBME facilitates the activities of international terrorist financiers, organized crime figures, and money launderers. For example, since at least early 2011, the head of an international narcotics trafficking and money laundering network has used shell companies' accounts at FBME to engage in financial activity. In late 2012, the head of the same international narcotics trafficking and money laundering network continued to express interest in conducting financial transactions through accounts with FBME in Cyprus. Separately, in 2008, an FBME customer received a deposit of hundreds of thousands of dollars from a financier for Lebanese Hezbollah. FBME also facilitates financial activity for transnational organized crime. As of 2008, a financial advisor for a major transnational organized crime figure who banked entirely at FBME in Cyprus maintained a relationship with the owners of FBME.

FBME facilitated transactions for entities that perpetrate fraud and cybercrime against victims from around the world, including in the United States. For example, in 2009, FBME facilitated the transfer of over $100,000 to an FBME account involved in a High Yield Investment Program ("HYIP") fraud against a U.S. person. In July 2012, the FBME customer operating the alleged HYIP was indicted in the United States District Court for the Northern District of Ohio for wire fraud and money laundering related to the HYIP fraud. FBME has processed payments for cybercrime networks. In September

2010, FBME facilitated the unauthorized transfer of over $100,000 to an FBME account from a Michigan-based company that was the victim of a phishing attack. Several FBME accounts have been the recipients of the proceeds of cybercriminal activity against U.S. victims. For example, in October 2012, an FBME account holder operating as a shell company was the intended beneficiary of over $600,000 in wire transfers generated from a fraud scheme, the majority of which came from a victim in California.

FBME's offshore banking business allows sanctioned entities to circumvent sanctions imposed by the International Emergency Economic Powers Act ("IEEPA"). IEEPA authorizes the President to declare the existence of an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States originating outside the United States. It further authorizes the President, after such a declaration, to impose sanctions, block transactions, and freeze assets to respond to the threat. FBME facilitates U.S. sanctions evasion through its extensive customer base of shell companies. For example, at least one FBME customer is a front company for a U.S.-sanctioned Syrian entity, the Scientific Studies and Research Center ("SSRC"), which has been designated as a proliferator of weapons of mass destruction. The SSRC front company used its FBME account to process transactions through the U.S. financial system. This SSRC front company also shared a Tortola, British Virgin Islands ("BVI") address with at least 111 other shell companies, including at least one other additional FBME customer that is subject to international sanctions.

FBME solicits and is recognized by its high-risk customers for its ease of use. FBME advertises the Bank to its potential customer base as willing to facilitate the evasion of AML regulations. Separately, FBME is recognized for the ease of its account

creation. In September 2013, FBME's offshore bank account services were featured prominently on a website that facilitates the formation of offshore entities. FBME is also popular with online gamblers, particularly U.S. gamblers that seek to engage in unlawful internet gambling. One website that encourages the opening of offshore bank accounts to gamble online notes that FBME in Cyprus is "[a]nother Europe-based bank [we've] found particularly easy to deal with."

In October 2011, the Department of Justice ("DOJ") filed civil forfeiture complaints against approximately $70.8 million in real and personal property alleged to be the proceeds of foreign corruption offenses perpetrated by the President of Equatorial Guinea, Teodoro Obiang's son and his associates and laundered through the United States. Subsequently, between December 2011 and July 2012, the Treasury of Equatorial Guinea wired over $47 million to several Cypriot banks and entities in a pattern of transactions that was identified as being consistent with the allegations in the DOJ complaint. This included $7.2 million wired to a British shell company using an FBME account.

**2. FBME's Weak AML Controls Encourage Use of the Bank by Shell Companies and Allow Its Customers to Perform a Significant Volume of Obscured Transactions and Activities Through the U.S. Financial System.**

FBME accesses the U.S. financial system through both direct and indirect correspondent accounts. In 2009, one U.S. financial institution terminated its banking relationship with FMBE based on money laundering concerns. The volume of suspicious wire activity conducted by FBME customers through the U.S. financial system, however, remains significant. In just the year from April 2013 through April 2014, FBME conducted at least $387 million in wire transfers through the U.S. financial system that

exhibited indicators of high-risk money laundering typologies, including widespread shell company activity, short-term "surge" wire activity, structuring, and high-risk business customers.

FBME has a significant number of shell company customers nominally based in Cyprus and in other high-risk jurisdictions. Wire transfers related to suspected shell company activities accounted for hundreds of millions of dollars of FBME's financial activity between 2006 and 2014. For example, FBME was involved in at least 4,500 suspicious wire transfers through U.S. correspondent accounts that totaled at least $875 million between November 2006 and March 2013. The FBME customers involved in these wire transfers exhibited shell company attributes, and other financial institutions involved in the transfers reported that they were unable to verify the identities of FBME's customers. A lack of transparency for such significant wire activity involving FBME's customers makes it extremely difficult for U.S. and other financial institutions involved in these transactions to verify the *bona fides* of all of the parties to these transfers.

FBME customers, including its many shell company customers, have frequently used FBME's Cyprus address to conduct collectively tens of millions of dollars of transactions. From July 2007 to February 2013, at least 71 entities used FBME's Cyprus address to conduct transactions through the U.S. financial system. Although there may be rare occasions when use of the bank's address as a bank customer's address of record is legitimate, such a practice is highly unusual and indicative of the bank's potential complicity in its customers' illicit activities. This is particularly true if a party to such a transaction is located in a high-risk or sanctioned jurisdiction. Obscuring the true address

of the customer inhibits compliance checks by counterparty or intermediary financial institutions.

## IV. The Extent to Which FBME Is Used for Legitimate Business Purposes in Cyprus and Tanzania

Legitimate activity at FBME's Cyprus branch is difficult to assess because of the limited amount of information that is available regarding Cypriot branches of foreign banks, such as FBME. FBME claims to have a relatively limited number of customers in Cyprus, yet it also states that it transacts over 90% of its global banking business, and holds over 90% of its assets, in its Cyprus branch. As discussed in this Notice of Finding, FBME functions largely as an offshore bank catering to a significant number of shell entities that are nominally located in Cyprus and other high-risk jurisdictions.

## V. The Extent to Which This Action Is Sufficient to Guard Against International Money Laundering and Other Financial Crimes.

FinCEN's [INSERT DATE OF PUBLICATION IN FEDERAL REGISTER] proposed imposition of the fifth special measure would guard against the international money laundering and other financial crime risks described above directly by restricting the ability of FBME to access the U.S. financial system to process transactions, and indirectly by public notification to the international financial community of the risks posed by dealing with FBME.

Dated: July 15, 2014.

Jennifer Shasky Calvery,
Director,
Financial Crimes Enforcement Network.

[FR Doc. 2014-17171 Filed 07/21/2014 at 8:45 am; Publication Date: 07/22/2014]