Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

September 22, 2014

BY ELECTRONIC FILING AND ELECTRONIC MAIL

Jennifer Shasky Calvery
Director
Financial Crimes Enforcement Network
U.S. Department of Treasury
P.O. Box 39
Vienna, VA 22183

Attention: Richard May, Director, FinCEN Office of Special Measures

Re: Notice of Proposed Rulemaking -- Financial Crimes Enforcement Network (FinCEN)

RIN 1506-AB27

Dear Director Shasky Calvery:

On behalf of our client, FBME Bank Ltd. ("FBME" or the "Bank"), we present the following comments with respect to the Notice of Proposed Rulemaking (the "NPRM") and Notice of Finding ("Notice") contained in RIN 1506-AB27, dated July 15, 2014 and published in the Federal Register on July 22, 2014.

FBME is committed to continuing to cooperate with the U.S. Government, as well as the governments of Cyprus and Tanzania, in the fight against money laundering and terrorist financing activities. FBME has devoted substantial resources to developing and enhancing its anti-money laundering ("AML") and sanctions compliance program ("Compliance Program" or "Program") to adhere to applicable European, Cypriot, and Tanzanian standards. Hogan Lovells LLP has retained Ernst & Young in the United States ("EY") to conduct a comprehensive, independent review of the Bank's Compliance Program and to make recommendations for improvement according to applicable regulatory standards and best practices. In its Assessment of FBME's Compliance Program dated September 22, 2014 ("Assessment"), which FBME will provide to FinCEN, EY observed that the Program "incorporates the requirements" of the EU's Third Money Laundering Directive (2005/60/EC) ("MLD3") and the fourth issue of the Central Bank of Cyprus ("CBC") Directive to credit institutions in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2013, issued in December 2013 (the "CBC 4th Directive") (together the "Directives") 1/ EY's Assessment further reported that FBME "has protocols in place that allow the Bank to continuously keep the Program aligned with these legal requirements." Hogan Lovells and EY have also made recommendations in some areas where FBME's Compliance Program "could be improved." FBME is already working to implement these

1/ We note that the requirements of the CBC 4th Directive exceed the requirements of the MLD3 The CBC 4th Directive is in line with the draft of the EU's proposed Fourth Money Laundering Directive, which has not yet been enacted.

recommendations, and the Bank will continue to enhance its Compliance Program to the satisfaction of FinCEN.

FBME has carefully reviewed the Notice and the NPRM. On the basis of this review and FBME's ongoing enhancement of its Compliance Program, FBME respectfully requests that FinCEN withdraw the Notice and the NPRM. Hogan Lovells respectfully submits that a complete review of the Bank's current Compliance Program and its plans for enhancing certain aspects of the Program will demonstrate that FinCEN should not impose the fifth special measure under Section 311 of the USA PATRIOT Act.

Rescission of the regulatory proposal here would be consonant with the purposes of Section 311. As the Department of the Treasury has noted, Section 311 special measures can spur rehabilitative conduct on behalf of the affected financial institution:

> "In some instances, the entities of primary money laundering concern have rehabilitated their practices and implemented significant reforms to mitigate some of the risks and vulnerabilities identified as supporting the finding of primary money laundering concern. In such circumstances where the continuing risks to the U.S. financial system appeared to be diminished, Treasury has decided not to pursue a final rule implementing special measures and notice has been given to rescind the regulatory proposal." 2/

At the outset of this comment, FBME wishes to make the following key points:

1. FBME's current Compliance Program incorporates the requirements of the Directives. FBME's compliance with these laws has been reviewed by EY and (also very recently) by KPMG AG WPG Frankfurt ("KPMG"). As described in section I.L.2. below, in 2013, KPMG determined that FBME's compliance policies were "comprehensive", and that the Bank's Compliance Program was "in principle in compliance" with the standards set by its regulators.

2. In response to program enhancement recommendations made by previous audits, FBME has substantially strengthened its Compliance Program over the last two years.

3. FBME and its officers and directors do not in any way condone the "use" of the Bank for illicit purposes and strive to prevent such misuse.

4. Some of the statements in the Notice are incorrect. Others appear to be based on incomplete information. FBME seeks to clarify these discrepancies in this comment and in its ongoing engagement with FinCEN.

5. In some cases, FBME filed a Suspicious Transaction Report to MOKAS (Republic of Cyprus' Unit for Combating Money Laundering) regarding events that appear to be related to those described in the Notice.

6. The Treasury Department's proposed rulemaking has had a significant adverse impact on the business activities of FBME and its customers and CBC's actions to place FBME

2/ U.S. Department of the Treasury, "Fact Sheet: Overview of Section 311 of the USA Patriot Act," (May 22, 2012), available at http://www.treasury.gov/press-center/press-releases/Pages/tg1591.aspx.

in resolution proceedings 3/ have not allowed the Bank to maintain its business. FBME's inability to function has, in turn, damaged the ability of thousands of FBME's business clients from operating their businesses. FBME therefore respectfully requests that FinCEN work with all appropriate dispatch in assessing FBME's response to the NPRM.

Section I of this comment describes FBME's Compliance Program. As EY found in its Assessment, "FBME's AML policies are in line with the applicable requirements of the Directives." The Bank's policies and procedures provide fulsome coverage of AML issues including KYC procedures, documentation for personal and corporate accounts, procedures for high-risk customers and approved third parties, monitoring of accounts and transactions, suspicious transaction reporting, employee training, and the role of the Money Laundering Compliance Officer. In January 2010, the Bank invested in industry-leading tools for transaction monitoring, employing Oracle's Mantas monitoring platform to review past transactions, and implementing CGI HotScan to screen all incoming and outgoing SWIFT transactions in real time against international sanctions lists. In March 2011, the Bank designated a new, highly qualified AML Compliance Officer and Global Head of Compliance, who has further invigorated the activities and increased the resources of the Compliance Department.

Section II of this comment addresses some of the specific statements in the Notice. This section responds to some statements in the Notice that are inaccurate, have been taken out of context, or require additional explanation. Unfortunately, FBME is unable to respond fully to other statements in the Notice because the Notice lacks information required for the Bank to identify the transaction(s) at issue, and the Treasury Department has not shared any additional information pertaining to the alleged transaction-specific activities with the Bank. The Bank takes seriously any allegation that its customers have used the Bank for illicit or illegal purposes. FBME looks forward to providing additional information to FinCEN and cooperating with U.S., Cypriot, and Tanzanian officials to halt any possible criminal or other illicit activities of third parties involving the Bank.

I. FBME'S ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

A. Overview of the Bank and the Program

FBME has been consistently operating in Cyprus for over 30 years. The Notices point out that during this time period, FBME has twice changed its country of incorporation. However, the Notices do not provide the context for these moves, which in both cases involved changing circumstances in FBME's country of incorporation that hindered FBME's ability to function as a legitimate international commercial bank.

In 1977, Michel Ayoub Saab and his son Ayoub-Farid M. Saab moved to Cyprus. Later that same year, the Federal Bank of Lebanon ("FBL"), a Lebanese retail bank owned by the Saab family, opened a representative office in Cyprus. Cyprus had close proximity to Lebanon, was a stable country, and had established good international communications networks.

In 1982, the Saab family sought to incorporate an international commercial bank in Cyprus. The CBC, however, was unwilling as a matter of policy to take on home supervisory responsibility over international banks that were not among the large international banks. Instead, the CBC required

3/ On July 18, 2014, the CBC announced that it was taking over management of the operations of the Bank's Cyprus branch. The Resolution Committee (appointed to manage the Bank) subsequently issued a Decree placing the branch under resolution and providing that the expressed purpose of the Decree was the sale of the Bank's operations in Cyprus.

the Saab family to establish its international bank in Cyprus as a subsidiary of a bank headquartered outside Cyprus. Accordingly, in 1982, the Saab family formed FBME (then named Federal Bank of the Middle East Ltd.) in Cyprus as a subsidiary of FBL, with fifty-one percent of the shares owned by FBL and forty-nine percent owned by Michel Ayoub Saab, Ayoub-Farid M. Saab, and Fadi M. Saab.

In 1985, security deteriorated in Lebanon due to the Syrian occupation. The Saab family, who are members of the Lebanese-Christian minority, became concerned about the possibility of the occupying power nationalizing Lebanese banks, including FBL, which had been occurring elsewhere in the region at the time. The Saab family therefore decided to protect FBME by removing FBL from its ownership structure. In 1986, Michel Ayoub Saab, Ayoub-Farid M. Saab, and Fadi M. Saab acquired FBL's fifty-one percent ownership interest in FBME. At that time, FBME and FBL became unrelated legal entities. FBME was no longer a subsidiary of FBL, and the two entities have remained separate to the present day, although they are both presently owned by Ayoub-Farid M. Saab and Fadi M. Saab.

In 1985, FBME discussed with the CBC its options for incorporating the Bank in a foreign jurisdiction and maintaining a Cyprus branch. The CBC expressed to FBME that it would be advisable if FBME approached the Cayman Islands Monetary Authority ("CIMA") for a full banking license. The CBC made the necessary introductions and the Saabs took steps to apply for a "Banking License B" for a Cayman Islands incorporated company, Federal Bank of the Middle East Ltd ("FBME-CY"), which would allow a fully operating branch then to be based in Cyprus. Consequently, in 1986 FBME-CY changed its country of incorporation and primary banking license to the Cayman Islands. FBME's international banking business operations remained in Cyprus.

With the approval of the CBC and CIMA, FBME therefore incorporated itself in the Cayman Islands, and the Cyprus operations became a branch of the Bank. In 1987, the Cyprus branch received a license from the CBC to carry out banking business in Cyprus. In 1991, Michel Ayoub Saab passed away, and Ayoub-Farid M. Saab and Fadi M. Saab inherited their father's shares and became equal owners of FBME.

FBME's decision to move its headquarters to Tanzania was not motivated by any attempt to escape Cayman regulation, as the Notice seems to suggest. In 2001, fifteen years after FBME was incorporated in the Cayman Islands, the Cayman Islands amended its banking legislation to require all banks headquartered in the Cayman Islands to establish a physical presence there or cease conducting business in the Islands after April 2003. 4/

CIMA viewed this change in the law as a requirement to have a substantial physical and management presence in the Cayman Islands, which would have involved at least one of the Saab brothers residing in the Islands. Given the Bank's international customer base (in particular its geographic spread) and the fact that its existing work force was located primarily in Cyprus, the Bank decided that it made little business sense to establish a substantial physical and management

4/ In April 2001, the Banks and Trust Companies Law (2001 Revision) was amended to require all banks that were not a subsidiary or branch of a bank licensed in a country or territory outside the Islands to establish a physical presence in the Cayman Islands by January 2002. In December 2002, the Cayman Islands Law was further revised so as to provide that a holder of a "B" license which is not a subsidiary or branch of a bank licensed in a country or territory outside the Islands, shall not after April 2003 carry on business in the Islands unless it has such resources (including staff and facilities) and such books and records as the Authority considers appropriate with regard to the nature and scale of the business.

presence in the Cayman Islands. It therefore, once again, became necessary for FBME to find a new jurisdiction from which it could obtain a "Home License."

By this time, the Bank had already been doing some business in Africa and had targeted the continent as a region for expansion. FBME investigated various countries and spoke with different regulatory authorities, including representatives from the International Monetary Fund and the World Bank while visiting the Central Bank in Tanzania. The opportunity arose in 2003 for FBME to acquire from the Bank of Tanzania certain assets of Delphis Bank, which the Bank of Tanzania then held in receivership. FBME did not acquire Delphis Bank, but purchased certain assets and assumed certain liabilities. CIMA enabled this process to be accomplished by extending the April 2003 deadline first to July 2003, and then again to September 2003. Neither of these two extensions was linked by CIMA to any change in the capital structure of the Bank.

FBME moved its headquarters to Tanzania, obtained a license from the Bank of Tanzania, and began operations on September 12, 2003. Due to these changes and the fact that its customer base was primarily from Europe and the Commonwealth of Independent States ("CIS"), the Federal Bank of the Middle East Ltd. formally changed and shortened its name to FBME Bank Ltd. on August 4, 2005.

FBME is headquartered in Tanzania 5/ and operates primarily in Cyprus, owing to its legacy connection to the island. FBME is the longest established international bank in Cyprus, having operated continuously on the island since 1982. As of July 15, 2014, FBME had 375 employees, including 225 in Cyprus. 6/

FBME has a geographically diverse client base of international companies and individuals located in more than fifty countries. The Bank specializes in international commercial transactions accommodating high net worth individuals' banking needs, ranging from portfolio management to payment solutions. Of FBME's current customers, approximately 33.2% of deposits are from Europe, 35.4% are from the CIS market, 13.0% are from Asia, 11.3% are from sub-Saharan Africa,

---

5/ The Financial Action Task Force ("FATF"), of which the United States is a member and cooperating and supporting nation, has found Tanzania's banking system to have sufficient AML/CFT controls in place. As FATF stated in a June 27, 2014 press release:

> "The FATF welcomes Tanzania's significant progress in improving its AML/CFT regime and notes that Tanzania has established the legal and regulatory framework to meet its commitments in its action plan regarding the strategic deficiencies that the FATF had identified in October 2010. Tanzania is therefore no longer subject to FATF's monitoring process under its on-going global AML/CFT compliance process. Tanzania will work with ESAAMLG as it continues to address the full range of AML/CFT issues identified in its mutual evaluation report."

FATF, "Improving Global AML/CFT Compliance: on-going process - 27 June 2014 (Tanzania)," available at http://www.fatf-gafi.org/countries/s-t/tanzania/documents/fatf-compliance-june-2014.html. The United States is an observer to the Eastern and Southern Africa Anti-Money Laundering Group ("ESAAMLG"), and Tanzania has been a member of the ESAAMLG since its inception in 1999. In fact, the ESAAMLG was launched in Arusha, Tanzania.

6/ FBME Card Services Ltd ("FBMECS") had employed an additional 105 people, but 75 of those were laid off in August 2014 due to the refusal by the Special Administrator (appointed by the CBC to administer the Cyprus branch while under resolution) to settle with card companies and local merchants, causing FBMECS to suspend all activity. FBMECS currently employs 30 people.

4.3% are from the Americas, 2.5% are from the Middle East and Northern Africa, and 0.3% are from other locations. In 2013, the Bank had assets (e.g. cash balances, customer loans, property, etc.) of approximately 2.78bn US Dollars; liabilities (e.g. customer deposits) of 2.6bn US Dollars and total capital and reserves of 173m US Dollars. FBME's prudent financial management has proven successful, allowing the Bank to maintain a healthy financial condition amidst recent financial crises both internationally and in Cyprus. As of July 18, 2014, FBME's Cyprus branch had a liquidity ratio of 104%.

FBME is committed to complying with the laws and regulations of the Bank of Tanzania and the CBC. The Bank's Compliance Program has evolved in response to developing legal authorities within Europe, including the EU's MLD3, as implemented in Cyprus by The Prevention and Suppression of Money Laundering Activities Law (which came into force in Cyprus on January 1, 2008) (the "Law"). The CBC subsequently issued local directives, most recently the CBC 4th Directive which sets forth specific policy, procedures and control systems that all credit institutions should implement for the effective prevention of money laundering and terrorist financing so as to achieve full compliance with the Law (as amended since 2008).

B. Anti-Money Laundering Compliance Policies

The Bank has an extensive Manual of Policies and Procedures (the "Manual") that includes a detailed Compliance section. According to EY's Assessment, the Manual "is in line with the applicable requirements of the [CBC and EU] Directives."

Adopted in its current form in October 2006, the Manual is provided to all employees and is available electronically on all employee computer desktops as a shortcut from the shared drive of all Bank departments. Compliance personnel annually review and revise the Manual to implement enhancements to the Bank's Compliance Program or as and when prompted by changes in legal and regulatory requirements, industry best practices, or the recommendations of internal or external audits. Since its adoption in 2006, the Manual has been approved by senior management and the Bank's Board of Directors at least annually and whenever there were changes to law or policy that required updates to the Manual.

The Manual's Compliance section provides detailed policies and procedures covering AML issues, including but not limited to: KYC procedures, required documentation for personal and corporate accounts, procedures for high-risk customers, monitoring of accounts and transactions, and the role of the Money Laundering Compliance Officer. Further discussion of these and other topics is below.

C. Money Laundering Compliance Officer

FBME's Board of Directors has appointed a Money Laundering Compliance Officer ("MLCO") to oversee the Compliance Program and to report regularly his or her assessment of such compliance to the Board. Following the retirement of her predecessor in March 2011, FBME's current MLCO took over the position with the benefit of her predecessor's assistance as an advisor for a short time period to facilitate a smooth transition and provide any necessary information and training.

The current MLCO received her M.B.A. from Harvard Business School and has over a decade of banking experience. She holds a diploma in Compliance from the International Compliance Association in the United Kingdom and has studied international law. She started working at the Bank in 2009 and in 2011 became the MLCO and Group Head of Compliance. As evidenced by the CBC correspondence approving her appointment in April 2011 and as noted by EY in its

Assessment, FBME's MLCO "has the requisite qualifications (e.g., knowledge, skills, experience) and seniority to discharge her duties."

The MLCO's duties include, among others, effective implementation of the Compliance Program. Thus, the MLCO oversees the provision of training to employees, and is responsible for assessing and managing the risks emanating from existing and new customers. The MLCO also serves as a first point of contact for AML regulators. The MLCO directs the submission of suspicious transaction reports to the appropriate authorities and the maintenance of a registry of all such reports.

The Compliance Department reports to the MLCO / Group Head of Compliance, who in turn reports directly to the Board of Directors. The MLCO / Group Head of Compliance has been a member of the Executive Committee, which is the most senior management committee in the Bank, since that committee was formed in 2012. The MLCO delivers an annual report on the state of the Compliance Program to the Board of Directors and the Executive Committee. The MLCO's report to the Board includes an overview of new measures implemented to comply with the CBC's applicable directives, the findings and recommendations of any new audit results, the number of suspicious transaction reports submitted to MOKAS with any particular trends identified, the number of suspicious transactions investigated by the MLCO for which no report was filed with MOKAS, preparation of any recent internal suspicion reports, the identification of any gaps in monitoring, due diligence or other compliance functions, a summary of key information related to high-risk customers, an update on AML employee training, and any other information necessary to keep the Board apprised of AML developments within the Bank. (Additionally, in her role as Group Head of Compliance, she reports to the Board semiannually on general compliance matters, including AML, for FBMECS and FBME's Tanzanian operations.)

In 2014, the Board appointed an Alternate MLCO to assist the MLCO with her duties or formally act in her place in the case of absence or illness. Before joining FBME, the Alternate MLCO worked in the credit department of Commerzbank in Berlin. She began working at FBME in July 2007 and has served in the Account Opening section assisting the Head of the section and the Compliance Department, where she is currently an Assistant Manager (in addition to her Alternate MLCO duties).

D. Compliance Department

FBME is committed to maintaining a compliance program in line with or exceeding regulatory requirements and industry best practices of comparably-sized, similarly-located banks. When it named its new MLCO in 2011, FBME empowered its MLCO with the authority and resources necessary to expand and enhance the Compliance Program.

FBME and its management welcome regular feedback from internal and external sources such as auditors, correspondent banks, and regulators in order to identify and implement any necessary program enhancements. In response to recommendations and requests by the CBC, internal and external auditors, and Compliance Department leadership, FBME has taken significant steps to bolster its policies, procedures, and practices and has dramatically augmented the Compliance Department's resources. FBME has steadily increased the size and capability of the Compliance Department, which has tripled in size in five years, from six employees in 2009 to eighteen employees in 2014.

The current Compliance Department consists of seasoned professionals who have broad experience across the Bank. They draw from their understanding of how other departments function in order to ensure a healthy, seamless relationship between the compliance and business functions. In June 2011, the MLCO restructured the Compliance Department to provide dedicated functions for specific

program requirements. The Compliance Department is presently divided into three units: the New Accounts Approval Unit; the KYC Due Diligence Update Unit; and the Monitoring Unit.

1. *New Accounts Approval Unit*

The New Accounts Approval Unit consists of three employees who review all applications for new accounts. For each account, the New Accounts Approval Unit is required to perform a full KYC/background review of the prospective customer in accordance with the Bank's policies, described below in section I.F. Before approving the account, the Unit considers the prospective customer's business activities and risk level to determine whether such an account is consistent with the Bank's internal policies and the CBC 4th Directive. For example, upon the recommendation of the Compliance Department, the Board banned the onboarding of Russian Politically Exposed Persons ("PEPs") in January 2013 in light of compliance risks.

2. *KYC Due Diligence Update Unit*

The KYC Due Diligence Unit consists of seven employees responsible for completing annual reviews of all high-risk customers. The Bank's policy is to review customers classified as normal risk every three years. The KYC Due Diligence Unit is required to obtain up-to-date KYC documentation as part of the review. In the case of corporate customers, the Unit will check that the customer remains of good standing (for example by requesting a Certificate of Good Standing or performing a company search); review the customer's business activities to ensure they align with its transactions; and perform World-Check searches, internet searches, and sanctions screening (which is conducted for the shareholding structure, including the ultimate beneficial owner(s)). Should the KYC Due Diligence Unit encounter any questions or concerns, it involves other compliance personnel, such as the MLCO, to determine what further action should be taken. These KYC reviews are described in more detail in section I.F below.

3. *Monitoring Unit*

The Monitoring Unit consists of seven employees responsible for regularly monitoring payments being processed through the Bank's accounts. The monitoring process encompasses several functions, including, but not limited to: monitoring of live payments by processing transactions through HotScan to signal any pending transactions warranting closer analysis by the Compliance Department; monitoring all card transactions; monitoring post-factum transactions through Mantas, which detects irregularities in past payments; monitoring all inward and outward transfers related to high-risk accounts, regardless of amount, through HotScan; and manual transaction monitoring for high-risk accounts with markers flagging transactions for manual review. The Monitoring Unit is also required to prepare daily cash and check reports to determine whether there were any cash deposits in excess of 10,000 Euro or withdrawals in excess of 15,000 Euro (or equivalent), in which case documentation supporting the deposit / withdrawal is requested from the customer. (Note: cash and check payments total only 0.3% of the total value of payments made and 0.8% of the total number of transactions.) In addition, the Unit is required to prepare numerous other reports, such as monthly reports to the MLCO analyzing cash deposit patterns, reports of accounts closed by the Compliance Department, and suspicious transaction reports to MOKAS.

E. Customer Acceptance and Know Your Customer Policies

FBME's policy requires the Bank to conduct a thorough KYC exercise, including obtaining documentation to confirm the customer's identity, and the Bank uses standardized account opening

forms to complete this process. For corporate accounts, such documentation is required for all parties, including shareholders with an interest over 10% of each entity up to and including the ultimate beneficial owner(s). Required documentation includes passports and certified true copies thereof (or other legal alternatives), references, proof of address, certificates of incorporation, statutory documents, and other items consistent with industry best practices. Individual customers complete an Activity Profile, and corporate customers complete a Business Profile, which contains information on the purpose for which the account is required; the anticipated annual account turnover and method of deposits; a detailed description of the customer's main business activities; the expected sources of incoming funds (including countries and principal counterparties); and expected destination of outgoing payments (including countries and principal counterparties). Further, since 2007, the Bank has used the World-Check® database to screen customers not only for sanctions exposure, but also to help identify reputational risk (the background check includes a search of adverse media). *See* http://thomsonreuters.com/world-check-risk-intelligence/. The Bank conducts its own KYC on all customers, even those referred by its most trusted Approved Third Parties ("ATPs").

Some aspects of the Bank's KYC practices exceed U.S. regulatory requirements. For example, consistent with EU best practices and CBC requirements, FBME has required the identification and verification of ultimate beneficial owners since at least 2000. FinCEN proposed just last month to require U.S. financial institutions to identify ultimate beneficial owners. 7/ Moreover, FinCEN's proposal sets a threshold of a 25% equity interest for the identification of ultimate beneficial owners. FBME adheres to a far stricter threshold, defining ultimate beneficial owners as "persons with direct or indirect ownership or control or voting rights of 10% plus one share of the company's share capital." 8/

EY's Assessment notes that, "FBME applies [Enhanced Due Diligence ("EDD")] measures on its high-risk customers" in accordance with the requirements of the Manual. The Compliance Department is required to classify customers as high-risk if they are: PEPs (public functionaries or related individuals who present higher risks for bribery and corruption due to their position); bearer share companies; trusts; foundations; non-face-to-face customers; customers from countries that do not apply FATF's Recommendations; correspondent banks outside the EU; or if they meet any of several other factors listed in the Compliance section of the Manual. FBME does not employ a one-size-fits-all approach to EDD for high-risk clients. Instead, as EY points out, EDD measures "are tailored to address the unique risk(s) posed by each . . . customer type." The Manual defines appropriate EDD measures, which may include, for example, completing Bearer Share Questionnaires (*e.g.*, to identify changes in corporate ownership structure), conducting a further analysis of PEP relationships (*e.g.*, additional background checks on the PEP focusing on source of wealth), and verifying the validity of business / professional licenses. All high-risk customers must be approved by the MLCO or Alternate MLCO prior to account opening.

FBME recognizes the importance of regularly reviewing its KYC procedures in order to eliminate any potential gaps and ensure the Bank utilizes evolving technologies. In its 2013 external audit of FBME (discussed below), KPMG noted that a Customer Relationship Management System ("CRMS") ought to be implemented to enable better oversight of all customer-related data, and the Bank did so in 2013. Similarly, KPMG recommended that FBME add specific markers in FlexCube

---

7/ *See* Notice of Proposed Rulemaking, Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151-74 (Aug. 4, 2014).

8/ FBME Manual of Policies and Procedures, § 3.2.3.2.

(FBME's core banking system) describing the nature of all high-risk accounts. The Bank also made this upgrade in 2013. (Previously, the version of FlexCube the Bank was using did not provide for the nature of the high risk to be identified in the system; it only allowed for the categorization of accounts as high-risk. However, the Compliance Department maintained spreadsheets which assigned specific categories to the high-risk accounts. The current version of FlexCube enables this categorization detail.)

KPMG also identified a limited number of customer files containing some expired due diligence documentation and, as a result, KPMG recommended adding a function to the Bank's automated system to alert compliance officers whenever a document expires. The Bank is in the process of implementing an alert functionality in the CRMS.

In September 2014, EY reviewed FBME's Manual and reported that FBME's policies, procedures, and processes are in line with the Directives. EY then tested a statistically relevant sample of recent and older corporate and individual customer files in order to determine whether the procedures are properly carried out in line with the Manual. For almost all of the reviewed customer files, FBME conduced sufficient due diligence and collected all necessary information from its customers.

EY identified certain enhancements FBME could implement, such as more consistently documenting its verification of the sources of funds/wealth and its internet and database searches for customer identification. FBME is enhancing its procedures in accordance with EY's recommendations.

F. Updates to Customer Due Diligence

As noted in section I.D above, FBME has a separate unit dedicated to reviewing and updating KYC. The team of seven officers is devoted exclusively to the updating and maintenance of customer files.

1. *All customers*

All customer files are reviewed regularly to ensure the adequacy and validity of relevant identification documents and information. The outcome of such review is recorded in a separate note kept in the customer file. Each non-high-risk customer file is reviewed every three years. Additional due diligence is undertaken whenever, for example, an individual transaction appears to be unusual or significant compared to the normal pattern of transactions or the business profile of the customer; there is a change in the legal status, corporate structure; or there is a change in the way the account operates. The Compliance Department maintains files that compare transactions executed against anticipated or usual turnover.

2. *High-risk customers*

FBME's Manual requires the review of high-risk customer files on an annual basis. Transactions executed are compared against anticipated or usual turnover (this annual comparison is kept on file). The KYC team also reconfirms the customer's business activities, location, and status as an entity in good legal standing and not subject to international sanctions.

In addition, certain types of high-risk accounts (such as accounts held for PEPs or companies with bearer shares, etc.) are subject to annual all-encompassing review by the Monitoring Team and approval by the MLCO or Alternate MLCO for continuation of the relationship.

PEPs must fill out a supplemental due diligence form, which probes their involvement in public administration as well as their professional background and source of wealth. The form also contains

questions about close associates and the visibility of immediate family members in public life. As stated above, for example, the onboarding of Russian PEPs has been prohibited since January 2013.

G. Approved Third Parties

In accordance with its applicable policies and procedures and as permitted by the CBC 4th Directive, the Bank engages certain ATPs to develop potential new customer relationships. FBME seeks lawyers, accountants, and other licensed professionals from trusted occupations who can refer potential customers, and who are subject to supervision with regard to their compliance with the requirements of MLD3 or are from selected jurisdictions determined by the Cyprus Advisory Authority for Combating Money Laundering and Terrorist Financing to have AML/CTF measures equivalent to those within the EU.

Business development personnel attend professional conferences to develop relationships with these potential partners. FBME recognizes significant value in utilizing licensed professionals to identify potential customers, and as a result, around 90% of the Bank's customers are introduced by ATPs. The Bank identifies potential ATPs through one of six ways: membership of a professional association; internet research; business magazines and newspapers; referral by existing associates or clients; attendance at conferences or seminars relating to tax planning or the offshore industry; or recommendation by FBME staff or an existing ATP.

1. *ATP Due Diligence*

The Bank's engagement with these ATPs is governed by its Manual. Upon identifying a prospective ATP, the Bank must ensure that the country of operation of the ATP falls within the target areas designated by the CBC 4th Directive. FBME then registers the ATP on a "prospective list" for record-keeping purposes. All ATPs must hold membership in a professional association that regulates and supervises the ATP for AML compliance.

Before engaging a new ATP, FBME policy requires that the prospective ATP complete a due diligence questionnaire. This questionnaire requests information about the regulatory environment surrounding the ATP; its customer acceptance, identification and verification policies; its record-keeping and reporting procedures; and its training program. The Bank reviews the ATP's AML/CTF policies to confirm they adhere to the Bank's requirements.

Additionally, all ATPs must complete a profile form. Prospective ATPs acting in a personal capacity must include general information, including their name, their business and correspondence addresses, and contact information. These prospective ATPs must also explain their business activities, including areas of expertise and industry sector. The prospective ATP must also provide information about their clientele, including nationality, industry sector, and net worth. In addition to all of this information, prospective corporate ATPs must provide additional information, including the names of all partners and directors, whether the ATP acts as a nominee director and/or shareholder, and detailed company information.

All prospective ATPs must also provide sufficient supporting documentation. Personal ATPs must provide: policies and procedures for preventing money laundering and terrorist financing, as noted above; a certified copy of a passport or national identification card; proof of residential address; a personal reference letter from a bank, lawyer, or chartered/certified accountant; and a regulatory license. Corporate ATPs must provide: the company's written policies and procedures for preventing money laundering and terrorist financing; a certified copy of statutory documents for the

corporate entity; a certified copy of statutory documents for any nominee companies; certified copies of passports for all directors, shareholders, and beneficial owners; proof of residential address for all directors, shareholders, and beneficial owners; reference letters from a bank, lawyer, or chartered/certified accountant for all directors, shareholders, and beneficial owners; and a regulatory license.

The Bank performs due diligence on all ATPs in accordance with the Manual, including contacting professional organizations to ensure that the prospective ATP is a member and is supervised for AML compliance purposes. The Bank also performs KYC of the ATP, including World-Check searches, URU passport verification, and internet searches. If the ATP clears all due diligence and KYC processes, the file is sent to the MLCO/Group Head of Compliance for final approval.

2. *MLCO Approval of ATPs*

If the ATP satisfies the requirements of FBME policy, the Group Head of Compliance may approve the engagement. According to EY's Assessment, "the MLCO assesses the adequacy of the third party by reviewing the ATP's policies and procedures." In all the ATP files that EY tested, the MLCO approved the ATP before it began a relationship with the Bank.

3. *ATP Contracts and Guidance Documents*

All ATP relationships are governed by the Bank's Business Introducer Agreement, with which ATPs must agree to comply. The agreement provides that the ATP must comply with all laws, rules, and regulations and may not refer any client which could violate any laws, rules, and regulations that might breach the terms and conditions of FBME's banking license, Cypriot law, the rules and regulations of the CBC, or FBME's internal policies and practices

FBME requires that the ATP ensure strict compliance with the Bank's customer identification and due diligence procedures for all clients. ATPs must continue to follow the Bank's updated identification and due diligence procedures whenever those procedures are amended by the Bank. The Bank further reserves the right to check and verify the due diligence performed by the ATP. The Bank may also refuse to accept any new clients referred by any ATP, terminate any clients referred by any ATP, and refuse further business from any ATP. The Bank may also terminate its relationship with any ATP. Notably, the Bank has terminated ATPs where the ATP has failed to satisfy the Bank's expectation for referring compliant customers. The Bank also declines to open new accounts for potential customers referred by ATPs when those customers fail to meet the Bank's compliance requirements. FBME welcomes the opportunity to provide more specific information on these points to FinCEN.

Additionally, the Bank provides each ATP with a document titled "Customer Acceptance – Guidance Notes," ("The Guidance"), which describes the types of business that FBME seeks and that which it does not permit. The Guidance provides that clients of the Bank are corporate entities or higher net-worth individuals actively involved in the international trade of goods and services, or managing their global wealth and assets. The document also specifically describes unacceptable client relationships. The form describes unacceptable clients in a number of categories: (1) certain clients, including persons or entities on US, EU, UK, and UN sanctions lists and anonymous accounts; (2) certain activities, including production or trade of weapons, gaming and gambling related business, adult entertainment, and unlicensed trade of pharmaceutical products; and (3) certain geographical locations, currently Iran, Syria, North Korea, Cuba, and North Sudan.

4. *Customer Due Diligence*

All of the Bank's customers are subject to the due diligence procedures required by the Manual. The Bank's policies permit it to rely on ATPs to implement certain customer identification and due diligence procedures. These procedures are generally limited to the ATP certifying customer documents as true copies of originals. In order to accept this data, the Bank also must confirm that the ATP implemented these policies in line with the requirements of the law and directives issued by the relevant supervisory authorities.

After the Bank opens an account, FBME's policies require the Bank to obtain all ongoing due diligence directly from the directors or beneficial owners on the customer's account. These policies prescribe the minimum standards Bank personnel may follow. In practice, the Bank performs complete due diligence for all prospective clients referred by ATPs, including performing World Check and internet searches. For example, when the Bank accepts certified copies of a customer's passport via an ATP, the Bank still confirms the authenticity of the document though an identify check in the URU database maintained by GB Global PLC.

5. *ATP Monitoring*

The Bank's Business Development Team maintains a close relationship with ATPs. Business development personnel regularly visit ATPs to cultivate the relationship, ensure the ATP understands the Bank's practices, and confirm that the ATP is operating as described in its ATP Profile. FBME employees are encouraged to contact the ATP at least every three months. FBME monitors ATPs annually not only in terms of the quality of the customers they introduce, but also the occurrence of account closures and suspicious transaction reports submitted to MOKAS. Their registrations or licenses are verified regularly to confirm validity. The MLCO further performs an annual reassessment of ATPs in accordance with the current Directive. In appropriate cases, the Bank terminates ATPs that do not satisfy the Bank's requirements.

H. Transactional and Account Monitoring

As noted above, the Compliance Department was restructured in 2011, resulting in the creation of a dedicated Monitoring Unit. FBME also has been consistently enhancing its Compliance Program through the introduction and use of electronic solutions in addition to the manual review of transaction and account activity. FBME uses automated monitoring systems that detect unusual or suspicious activities or types of transactions by setting limits on certain types of transactions or categories of accounts, while considering the customer's business profile, country of origin and source of funds, nature of transaction, and other factors.

1. *HotScan*

Since January 2010, FBME has used the CGI HotScan Intelligent Self Learning sanctions screening solution, an interdiction filter that monitors the Bank's outgoing and incoming SWIFT transactions in real-time (*see* http://www.cgi-group.co.uk/solutions/HotScan). HotScan screens all payments against current sanctions lists from the U.S. Department of Treasury Office of Foreign Assets Control ("OFAC"), the United Nations, the EU, HM Treasury (UK), and other regulatory bodies, as well as lists maintained by financial agencies such as the Financial Action Task Force, the Financial Conduct Authority (UK), the Cyprus Securities and Exchange Commission, and others. The lists are updated daily from their sources and uploaded into HotScan. HotScan also enables manual entry of individuals and internal watchlists, such as lists of high-risk accounts, into the system. In addition to

the above, HotScan stops all inward/outward transfers as per the value thresholds set in the system (500,000 Euro and 100,000 US Dollars or equivalent in Tanzania) for investigation and so that documents can be obtained before processing. Although HotScan does not review internal transfers between existing Bank client accounts, the Compliance Department generates a report of and reviews manually such transfers on a daily basis.

Transactions that contain a positive match to HotScan's list are put on hold (i.e. frozen and reported or rejected, depending on the nature of the match). Partial matches trigger an investigation, and the payment will be processed only in the event of a false positive match. The investigation may include obtaining supporting documents such as contracts, invoices, bills of lading, etc., as well as a review of the account holder's past activity, information regarding the account holder's ultimate beneficial owner(s), internet search results, and additional documentation sought from the account holder. For outgoing payments, two different investigators must review the alert, and HotScan has a control in place to ensure this double-review takes place. All alerts are documented in an Excel spreadsheet.

2. *Mantas*

Since January 2010, FBME has also used Oracle's industry-leading Mantas AML monitoring platform, which evaluates past transactions and tracks the following pre-populated scenarios: fund transfers between customers and external entities, focal high-risk entity, high-risk counterparty, rapid movement of funds, large depreciation of account value, and large reportable transactions (*see* http://www.oracle.com/us/industries/financial-services/mantas-anti-money-laundering-ds-046161.pdf). Up-to-date transaction and account information data from the core banking system, FlexCube, is imported into Mantas, which runs an automated script to detect any activity under these scenarios and generate an alert if there is such activity.

If an alert is generated, FBME Compliance staff conducts an investigation, which is tracked and documented in an Excel spreadsheet. An investigator may draft an internal report or may add a "marker" to an account, which will notify personnel monitoring accounts when the client attempts to transact further. The monitoring personnel can then review the transaction or request further information from the client before any transaction is processed. If a decision is taken to close an account, a marker is placed on the account to indicate this decision. FBME promptly notifies the client and terminates the relationship within the minimum notice period required by law.

Although FBME has adequately tracked alerts and their investigation and disposition in Excel spreadsheets, EY recommended that the Bank introduce an automated system to perform these tasks. An electronic case management system would register alerts, track the progress of the related investigation, and automatically update the report when an investigation was closed. It would also generate case reports. FBME plans to introduce this system by the end of 2014.

3. *Manual Review*

In addition to utilizing electronic resources, the Compliance Department manually reviews a list of cash and check transactions on a daily basis, and retains transaction records and supporting documentation in hard copy format. Documentation of the source of funds is required for deposits over 10,000 Euro which have historically been and still are at very low levels due to the non-retail model of the Bank. Withdrawals of over 15,000 Euro require a stated purpose and over 30,000 Euro require documentation that justifies the economic / business purposes of such withdrawals.

Monthly reports of cash and check transactions are also kept in the same file and are reviewed for patterns of suspicious activity, in conjunction with the previous three months' activity.

I. Suspicious Transaction Reporting to MOKAS

The Bank has an effective process to escalate suspicious activities to the MLCO and (where appropriate) to MOKAS. Thus, after EY reviewed this process, it made no recommendations for improvement. When the Compliance Department is investigating a customer for suspicious activity, the Bank places a marker on the relevant account to denote that the customer is under investigation. If the Compliance Department determines that a customer's activities are suspicious, the MLCO prepares a Suspicious Transaction Report ("STR") and files the report with MOKAS. The Bank maintains a spreadsheet of all STRs that have been filed with MOKAS. The Bank keeps a copy of the STR, MOKAS' acknowledgment of receipt, and the disposition of the STR by MOKAS. If it does not receive a response from MOKAS within 14 days, the Bank will close the client's account unless otherwise advised by MOKAS. The Bank has engaged with MOKAS on a regular basis, and its relationship with MOKAS is characterized by frequent communication and swift resolution of concerns. On multiple occasions, MOKAS staff has verbally complimented FBME employees on their helpfulness and cooperation.

J. Training

Bank employees, including those in back office and support functions, receive training relating to compliance matters, including AML and sanctions policies and procedures. Employees maintain a "Training Passport" containing stamps for each training session that they attend. These trainings consist of on-site and off-site programs. In 2004, the Head of Compliance and Audit created an education plan for all Bank employees. According to Bank policy, all newly hired employees are required to receive initial induction training featuring these AML and sanctions-related topics. Under current procedures, the MLCO conducts these trainings on an ad hoc basis. Consistent with EY's recommendation, the MLCO is documenting a formal induction training curriculum for all new employees.

The trainings cover both high-level AML concepts as well as procedural and substantive issues. To ensure that participants actually process the material instead of simply passively absorbing it, quizzes and other interactive exercises are given to confirm mastery of the content.

Furthermore, supplemental training is provided to customer-facing employees in accordance with the CBC 4th Directive. For example, on July 12, 2014, FBME held AML training at the Hilton Hotel in Nicosia, Cyprus, signaling the importance of the subject matter and differentiating it from a routine information session on Bank premises. In this session, the MLCO provided training on the changes in AML law and the CBC 4th Directive to all staff in customer-facing departments. EY reviewed the July 12, 2014 training provided to customer-facing employees. EY determined that the content met the key requirements of the Directives and addressed the following subjects, among others: customer due diligence / customer acceptance, handling of PEPs and other high-risk customers, ongoing monitoring of customer relationships, updating customer records, and reliance on third parties (e.g. key business introducers). The Bank also conducted a more general AML e-training for staff employed in the back office and support functions. FBME had also been planning a September 2014 general knowledge training course for all Bank employees, but this has been delayed since the installment by the CBC of a Special Administrator over the Bank.

This supplemental training is also combined with interface between groups so that other departments within the Bank can gain visibility into daily compliance functions. For example, in March 2013, a team of employees from the Client Relationship Management Unit spent a half day in the Compliance Department during the course of a business day in order to better understand routine compliance functions and activity.

All employees within the Compliance Department also have attended external AML trainings, including those offered by other institutions, to stay informed about key regulatory developments and industry practices. For example, four employees (including employees from FBMECS) attended a December 2013 seminar held by KPMG that covered changes to AML requirements under the CBC 4th Directive and the impact of those changes on Cyprus. FBME also sent an employee to the Association of Certified Anti-Money Laundering Specialists AML/CTF seminar and workshops in London in May 2014, as it has done in several years past. The MLCO maintains a Training Register that documents past trainings (2012-2014) taken by Compliance staff. In accordance with EY's recommendations, FBME is working to implement a streamlined system to replace the Training Register as a method of documenting these trainings. FBME will be pleased to provide more information to FinCEN regarding the nature and content of the Bank's training.

K. Risk Assessment

Following the advice of KPMG discussed below in section I.L.2, the MLCO enhanced the Compliance Program by creating a formal AML/CTF risk assessment in addition to the Risk Department's assessment of operational risk. This first AML/CTF risk assessment of FBME's Cyprus branch was completed in February 2014.

The AML/CFT risk assessment examined risks posed by the following areas: the Bank's customers; customers' behavior; distribution channels; the Bank's products and services; the nature and profile of customers, nature of business transactions and products and services offered; the customers' geographical location and the origin and destination of customers' funds; the scale and complexity of the Bank's operation and geographical spread of its operations, staffing of compliance department, storage of KYC data and record retention; and deviations from the anticipated level, volume and size of transactions from the stated business activities of customers. The MLCO assessed several potential risk areas within each of these broader categories, ultimately investigating approximately fifty-five areas of potential risk. The assessment determined that additional controls were unnecessary for fifty of these potential risk areas and identified five areas requiring follow up.

First, the risk assessment concluded that additional control measures ought to be applied to accord with newly issued CBC guidelines regarding PEPs. The assessment found that PEPs are identified through World Check and internet searches, and the Bank performs full checks to ensure that the PEP has not been involved in any cases of corruption, embezzlement, etc. and does not have any criminal track record. The Bank also requires the Head of Compliance to sign a PEP profile document, and twice yearly reviews of PEP customers are conducted by the AML Monitoring and KYC Due Diligence teams. All PEP transactions are closely monitored. The risk assessment generally suggested additional control measures relating to the identification of source of wealth and funds for PEPs, and FBME implemented them in March 2014, earlier than the suggested due date of mid-2014.

The risk assessment also found that the Bank refuses all potential non-face to face customers as defined in the Directives, including any customers approaching the Bank via telephone, internet, or mail. The very few non-face-to-face customers are categorized as high risk, such that all transactions are closely monitored. It has always been the Bank's business model not to accept customers who approach the Bank via telephone, internet or mail, and the Bank has only five non-face-to-face customers, all of whom were recommended by existing clients. The risk assessment recommended that efforts be undertaken on an ongoing basis to make all such relationships face-to-face.

Additionally, the risk assessment concluded that the majority of the Bank's customers are introduced by ATPs, but that any risk associated with this is mitigated by having the accounts approved by a unit reporting to the Head of Compliance, who reserves the right to reject any account application. In addition, should ATPs fail to introduce quality customers, the ATP is subject to termination. As noted in section I.G.4, the Bank does due diligence on all customers referred by ATPs. The MLCO has declined to open accounts for customers who did not provide complete documentation or where the due diligence otherwise triggers compliance concerns. In addition, the MLCO has terminated relationships with ATPs for referring potential customers who fail the due diligence process. FBME is happy to provide further detail to FinCEN regarding these account declinations and ATP terminations.

The risk is further reduced by FBME's use of a document called the Customer Acceptance – Guidance Notes, which lists the type of business the Bank seeks (always subject to the customer meeting the Bank's due diligence requirements). The Bank also circulates to all ATPs a list of unacceptable activities, jurisdictions, and types of client. Many customers also visit the Bank or are visited by members of FBME staff at the onset or during the course of the relationship. The risk assessment recommended making ongoing efforts to see more customers in person. The Bank's practice is to meet all customers who have balances of more than 100,000 US Dollars (or equivalent) in person, although Bank personnel also meet other clients with smaller balances.

The risk assessment further found that all fiduciary loans are co-signed by the Head of Credit and the Head of Compliance after they pass compliance screening and due diligence checks. The MLCO recommended that the Bank gradually reduce the number of fiduciary customers by mid-2015. The Bank has recognized this recommendation and the number of fiduciary customers has been reduced since.

The AML/CTF report has been discussed both at the Executive Committee and Board of Director meetings and approved by both bodies. FBME was pleased to see that potential risk areas continue to be effectively mitigated. However, the Bank takes seriously the recommendations for additional controls made by its MLCO and continues to take steps to work to reduce its risks.

L. Recent Third Party Reviews of FBME's Compliance Program

FBME has benefited from the findings and recommendations of the third party auditors that have reviewed its policies and procedures. EY reports in its Assessment that "All previously identified money laundering and sanctions-related issues have been addressed by the institution. For those corrective actions that have yet to be fully implemented, FBME has documented project plans with milestone dates in place." FBME's work to implement or improve procedures relating to the areas identified in past audit reports is described below.

1. *Ernst & Young audit (2011)*

In 2011, EY released the results of an audit that consisted of reviewing AML policies, procedures, reports, and other related documents; interviewing senior Bank employees; and reviewing 95 customer files selected by the Bank's Compliance Department (the "EY 2011 audit"). The goal was to assess whether the documents that FBME's Cyprus branch obtained during the client acceptance process as part of the Bank's KYC and due diligence work were consistent with the CBC Directive in existence at the time.

The EY 2011 audit noted that the standard Business Profile in use at the time for all new accounts included all the required information sufficient to meet the requirements of the CBC Directive. EY

noted that older versions of the Business Profile template used at different points in time did not have all of the required information. The EY 2011 audit noted that the Compliance Department had advised that it used the (then) current standard Business Profile as part of process of updating the information for existing customers.

The EY 2011 audit also reviewed whether FBME obtained appropriate documentation, including company incorporation documents, passports, and utility bills, and ensured that the certifications of such documents were valid. It noted that in certain cases incorporation documents for corporate customers, and passports and utility bills for individuals, were not appropriately certified, due in part to requirements of the CBC, which did not hold apostille to be an acceptable means of certification. The EY 2011 audit noted that the Bank compared actual against anticipated turnover for high-risk customers but observed that there was no evidence in non-high-risk files that actual transactions executed were being compared against anticipated or usual turnover on the account. The EY 2011 audit report further noted that the comparison of anticipated and actual turnover was being done annually by the Bank's Compliance Department for all clients, using an automated report extracted by the Bank's system.

2. *KPMG audit (2013)*

In April 2013, KPMG released the results of an audit that consisted of reviewing documentation (including 68 customer files and two bank files selected randomly from lists of new and/or high-risk customers), walkthroughs, interviews with Bank personnel, and an assessment of the Bank's AML/CTF policies, procedures and practices. The goal was to assess whether FBME's AML/CTF policies and practices were compliant with EU and Cypriot law, as well as in accordance with good industry practice in Europe.

The review concluded that "FBME basically fulfills requirements as set out by the Cyprus regulator and is in principle in compliance with EU standards." KPMG found that FBME employed AML-compliant procedures, including using standardized account opening forms, assigning risk ratings to customers, verifying customer and UBO information, and performing database searches on all customers, and that the Bank's internal policies were comprehensive. KPMG also made a number of suggestions to further improve the Bank's Program. In addition to the enhancements described above (i.e., hiring an alternate MLCO and amending the Manual), the Bank has also focused on addressing other recommendations as well as the broader categories of concerns described below.

KPMG made observations, including those related to the accessibility of ownership information, documentation of information, and risk assessment. KPMG noted, for example, that FBME's core banking system (FlexCube) does not capture the names of UBOs. Instead the Bank stores that information in an Excel file that is screened on a monthly basis and as and when there are changes in current sanctions lists of designated parties (e.g. OFAC, EU, HMT). The spreadsheet can be accessed by middle and senior management in Compliance, IT, Audit, and Customer Service Departments, and has been screened regularly since 2011. KPMG also recommended better presentation of ownership information to demonstrate links between group entities for older customers, in line with a new structure that had been introduced for new customers. KPMG also found that certain customer files reviewed did not have sufficient information to gain a complete understanding of the customers' activities or business rationale. In response to such findings, FBME has increased its efforts to document the information obtained and reviewed.

Although it found that the Bank's strategy addressed a number of risk-related issues, KPMG recommended rethinking the approach to money-laundering and terrorist-financing to develop a

comprehensive risk analysis. As described above in section I.K., the Bank has adopted the AML/CTF risk assessment report and implemented this recommendation.

M. FBME Card Services

FBMECS was founded as a subsidiary of FBME Bank in 2002 to offer a range of charge card-related products and services to businesses. A member of VISA Europe and MasterCard International, FBMECS provides acquiring, issuing, and processing services to merchants across Europe, enabling them to authorize, settle, and manage transactions. FBMECS's card products include payout, payroll, and co-branded programs. FBMECS also offers related operational support for its customized processing services.

FBMECS has a separate AML Compliance Program, which has been audited multiple times by several independent auditors. Recent reports have praised FBMECS' "strong commitment to compliance" and noted that "past problems have been successfully remediated" (SightSpan, 2013). A 2014 RiskSkill audit that measured FBMECS policies and procedures against VISA standards gave resoundingly positive reviews to the program; in fact, RiskSkill stated that FBMECS had "overcompensated" for past failings, "driven by a strong compliance team/function and clear leadership directing [its] approach." A Deloitte audit, also in 2014, found that FBMECS was in compliance with Cyprus' requirements for a License to Operate an Electronic Money Institution, stating that the company had in place correct and appropriate management and accounting procedures, had sufficient internal control mechanisms, and had taken all auditing and governance arrangements necessary to ensure reliable issue of electronic money.

The Bank acknowledges that it has had prior gaps in the AML program of FBMECS and has been fully committed to closing those gaps. FBMECS voluntarily sought the suspension of its VISA e-commerce license while it addressed these issues, and audits in 2012 identified the specific gaps in the program. In response, FBMECS implemented the recommendations of its auditors, including updating its customer files and creating an additional weekly report monitoring transactions above a certain threshold. In light of what it called "the significant progress made since May 2012," VISA had in turn reinstituted FBMECS' e-commerce license to acquire merchants on a provisional basis in June 2014. These substantial efforts and progress in 2014 took place prior to the issuance of the NPRM.

Not only has FBMECS continued to enhance its compliance program, but it also restructured the management of the company from 2012 to 2014, including in 2012 replacing the CEO who had led the company during the period in which there were (FBMECS accepts) compliance gaps. Prior to the issuance of the NPRM, the new leadership of FBMECS had been committed to the rigorous compliance program described in recent audit reports, had been well-reviewed by auditors, and had continued to enhance its compliance program. FBMECS also had named a new MLCO with extensive experience and other qualifications. The current FBMECS MLCO earned an M.B.A. from Hawaii Pacific University and spent one year as an operations specialist at an investment bank in New York. He then joined FBME, where he spent more than seven years, working his way up to Anti-Money Laundering Manager and Assistant MLCO before moving to FBMECS.

FBME would be pleased to provide further information on this subject.

II. LACK OF CONTEXT AND CERTAIN INACCURACIES IN FINCEN NOTICE

As stated above, FBME believes that the Notice contains a number of points purporting to justify the NPRM that are inaccurate, are taken out of context, or are less relevant with additional explanation.

We appreciate FinCEN considering this additional information. We will be pleased to provide further support for the points in this comment and to take all necessary steps to resolve these matters. The Notice statements addressed below include references to the Notice as it appeared in the Federal Register Volume 79 on Tuesday, July 22, 2014.

A. Statements in the Notice regarding FBME

FBME's preliminary responses to certain statements in the Notice are set forth below.

1. *Notice Statement: "The Central Bank of Cyprus ("CBC") . . . has found FBME's compliance with Cypriot banking laws and AML regulations deficient on at least two occasions." 79 Fed. Reg. 42639 (July 22, 2014)*

FBME strives to comply with all requests of the CBC. There have been two occasions where FBME was held to be not entirely compliant with CBC demands. In both circumstances, however, FBME openly communicated to the CBC its difficulties and objections to these demands. FBME continued to attempt to engage in dialog to avoid these issues.

a. Notice Statement: "FBME's weak AML controls and customer due diligence resulted in a fine by the CBC in 2008." 79 Fed. Reg. 42639 (July 22, 2014)

FBME was not fined by the CBC in 2008. In 2010, the CBC imposed an administrative fine on FBME. Following one of its regular on-site examinations of FBME, in March 2009 the CBC identified certain issues requiring corrective action including: making amendments to the Manual's customer identification processes; implementing an electronic management information system for monitoring accounts and transactions; and updating customer due diligence files. FBME immediately began addressing these issues. Among other measures, in April 2009 the Bank informed the CBC that it planned to amend its Manual and that it planned to install and implement Mantas by the end of June 2009 (which, following technical delays, went active in January 2010). As explained in detail below, the Bank further worked diligently to update its customer due diligence files. FBME kept the CBC informed of its progress. Throughout the process, the Bank closed the accounts of those dormant clients who declined to provide certified updated documents. Although the Bank ultimately failed to meet the CBC's deadline for updating its files because it did not receive all its customers' responses in time, it did complete its review of all files and requested the necessary documents from its customers before the deadline passed.

In March 2009, the CBC wrote to the Bank following one of its regular on-site examinations of the Cyprus branch. As part of its examination, the CBC had reviewed a sample of customer files and had identified areas for improvement with respect to the KYC information held on certain files. By way of example, the CBC felt that, in some cases, the information collected with respect to the customers' business activities or the occupation of UBOs was too broad. As a result, the CBC made certain recommendations to the Bank. It required the Bank to take steps to rectify the deficiencies which it had identified across the sample files, and to institute procedures to review and update customer files more generally. The Bank responded in April 2009 and confirmed that it would review and update its customer files as requested. Over the course of the following months, the Bank met with and wrote to the CBC to keep it informed of progress.

In December 2009, the CBC imposed a deadline of March 31, 2010 for completion of the review and update of all customer files (regardless of risk rating or dormancy). Given the size of the project, the Bank promptly informed the CBC that it would not be able to meet the deadline and sought a short

extension of time. Its request was refused. In late January 2010, the Bank wrote to the CBC and confirmed that it had fully reviewed and updated the sample of customer files identified during the 2009 on-site examination and that it was continuing to review and update the balance of its customer files. The Bank noted that it had ten employees working intensively (including nights and weekends) to complete the task and was making every effort to meet the CBC's deadline. However, the Bank explained that it had to review approximately 9,000 files and that the project was time-consuming, in particular because many of the Bank's customers were located abroad. The CBC did not permit FBME to accept certified identity documentation through apostille and notarization for international customers, instead requiring documents certified either by a bank officer or an ATP from all of FBME's many international clients.

Notably, the Bank was able to complete its review of all files and contact all relevant customers by the deadline set by the CBC, but it did not receive all updated records by the deadline. On March 31, 2010, the Bank told the CBC that, despite its best efforts and serious commitment, it was unlikely to complete the task before the end of June 2010.

In November 2010, the CBC imposed an administrative fine. FBME notified the CBC in September 2011 of the actions taken to address the areas for improvement identified by the CBC. The CBC next conducted an on-site examination in November 2011 where they reviewed, *inter alia*, a large sample of customers of different types, risk-rating, and on-boarding in different years. The CBC did not identify any further concerns with respect to the customer identification issues referenced in its 2009 on-site examination.

b. Notice Statement: "[I]n 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." 79 Fed. Reg. 42639 (July 22, 2014)

This statement is neither accurate nor supported by credible sources. FBME never sought to evade oversight by the Cypriot regulatory authorities. Rather, it consistently and promptly communicated with the CBC in real time about the payments affected by capital controls directives at issue. The CBC never stated that FBME may be subject to a fine of up to 240 million Euro; the only support for the statement in the Notice is a November 2013 article in the Cyprus Mail relying on "sources at the central bank . . . who wished to remain anonymous." 9/ We note that it is a criminal offense in Cyprus for a CBC employee to leak confidential bank information gained through CBC employment. When the CBC did eventually impose a fine, it was for reasons totally unrelated to AML issues, the fine was approximately one quarter of one percent of the amount referenced in the article, and it is being disputed by FBME in the Supreme Court of Cyprus on the basis that it is legally infirm.

In early 2013, Cyprus experienced a financial crisis. In mid-March 2013, the CBC suspended the payment system until further notice and then declared a series of consecutive bank holidays (effectively closing the banks). When banks reopened on March 28, 2013, the Minister of Finance (following the recommendation of the Governor of the CBC) issued the first of a series of Restrictive Measures Decrees ("Decrees"), imposing blanket capital controls on all banks operating in Cyprus without regard to any particular bank's liquidity and capital stability. At the time of these Decrees, FBME was entirely solvent and posed no risk to the financial system. In fact, during the crisis,

---

9/ "CBC threatens FBME with €240m fine," Elias Hazou, Cyprus Mail (Nov. 29, 2013), available at http://cyprus-mail.com/2013/11/29.cbc-threatens-fbme-with-e240m-fine/.

FBME loaned the Republic of Cyprus over 200 million Euro, evidencing its stable financial conditions and its willingness and readiness to support the Cypriot economy. The early Decrees required all banks, including FBME, to obtain approval from a designated committee of the CBC ("CBC Committee") for any transfers of money out of Cyprus. The Decrees required the CBC Committee to approve or decline banks' payment requests within 24 hours of receiving the request. On March 16, 2013, the Association of International Banks (the "Association"), on behalf of FBME and its 25 other member banks, sent a letter to the CBC, stressing that foreign banks should be exempt from the Decrees' restrictions because, among other reasons, the foreign banks did not have the liquidity problems of the local Cypriot banks. The Association sent a similar letter to the Governor of the CBC on March 24, 2013.

Following the twelve-day suspension of business, FBME began sending transfer requests to the CBC Committee. The CBC Committee repeatedly failed to respond to FBME's requests in a timely fashion. The CBC Committee regularly missed the deadline, and in some cases the CBC Committee never responded at all. As a result of the CBC Committee's inaction, on April 3, 2013, FBME wrote to the Governor of the CBC, explaining that the Bank had not received any responses to its payment notifications within the time limits prescribed by the Decree.

On April 5, 2013, FBME wrote to the Cyprus Minister of Finance that the Decrees' restrictions were damaging its business and exacerbated the risk of capital flight from Cyprus. The Bank therefore requested a suspension of the Decrees with respect to FBME. FBME also notified the CBC that it would not comply with all of the Decrees' requirements with respect to certain international customers. In a letter to the Minister of Finance on April 5, 2013, FBME explained that it would "notify, but not seek the permission or approval of, the [CBC] on transaction dates and amounts" for international clients. However, FBME explained to the Ministry of Finance that it would employ a process to comply with the Decrees' objectives to prevent capital flight from Cyprus. Among other things, this process included FBME's refusal to transfer its Cypriot clients' money out of Cyprus. FBME also refused to open any accounts with funds transferred from other Cypriot banks. In addition, the Bank submitted to the CBC all the liquidity and solvency reports required by the Decrees, and it notified the CBC of its daily transactions affected by the Decrees. The Ministry of Finance did not respond to FBME's proposal.

After providing this clear written notice to the CBC and the Ministry of Finance, from at least April 30 through August 16, 2013, FBME promptly informed the CBC in writing about all of its payment transfers out of Cyprus. FBME also sent numerous letters to the CBC and continually offered to meet in person to discuss the CBC's concerns, if any, with FBME's proposal. The CBC never responded to FBME efforts to communicate. FBME interpreted the CBC's silence as approval of the Bank's proposal. During this period, FBME's deposit base increased by 3%, consistent with the aims of the Decrees.

As noted above, FBME is unaware of any public statement by the CBC that it considered imposing a 240 million Euro fine on the Bank; however, FBME is aware of the single Cypriot newspaper article reporting that anonymous sources purporting to be from the CBC had said that the Governor of the CBC had discretion to decide whether to impose such a fine. 10/ On February 28, 2014, the CBC issued a decision imposing a fine on FBME of 652,320 Euro for these alleged violations. Immediately thereafter, FBME filed an application before the Supreme Court of Cyprus for administrative review of the fine because the CBC's application of the Decree violated Cyprus law

10/ "CBC threatens FBE with €240m fine," Elias Hazou, Cyprus Mail (Nov. 29, 2013), available at http://cyprus-mail.com/2013/11/29.cbc-threatens-fbme-with-e240m-fine/.

and the constitution and European law. FBME continues to litigate this matter in the courts of Cyprus, is seeking to refer the matter to the European Court of Justice, and is confident that it will ultimately prevail on the merits.

Throughout this process, FBME actively sought to maintain constructive dialogue with the CBC and the Ministry of Finance, but those agencies declined to respond. The Bank then openly communicated its plan to satisfy the objectives of the Decrees. Regardless of the outcome under Cypriot and EU law, we respectfully submit that FBME was not seeking to "evade oversight" by its regulator.

2. *Notice Statement: "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." 79 Fed. Reg. 42639 (July 22, 2014)*

FBME has controls in place that are audited annually by its regulator, the CBC. The CBC has not identified to the Bank a single case in which FBME facilitated any of the above activities. As described in more detail below, FBME is not aware that it is being "used" in this manner. If it is in fact being used in connection with money laundering or other illicit activity, the Bank is not knowingly or intentionally participating in such activities. The Bank might have been the victim of sophisticated criminal activities, notwithstanding the Bank's serious efforts to detect and prevent such activities. FBME would welcome the opportunity to review the evidence in the possession of the Treasury Department, to provide additional information, and to take action, together with U.S., Cypriot, and Tanzanian officials, to prevent any criminal activities. FBME remains ready, willing, and able to work with any regulator to ensure that such activities are not facilitated.

3. *Notice Statement: "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." 79 Fed. Reg. 42639 (July 22, 2014)*

Cyprus' favorable tax and fiscal environment attracts many businesses to establish asset holding companies that take advantage of the double tax treaties with almost 50 countries (*See* www.mof.gov.cy). This business climate explains why many of FBME's customers are holding companies, businesses with nominee structures, or "brass plate" companies with addresses in Cyprus. It is not uncommon for banks to service these types of companies; indeed, favorable Cypriot banking laws attract such customers. As set forth in the Bank's policies and procedures, upon the opening of an account, FBME collects information (from all customers) that is designed to ensure that the Bank knows the identity of its accountholders and the beneficial owners of those accountholders and ensures that accounts are not used for illicit purposes. In particular, the Bank has policies and procedures in place that are designed to identify customers that pose "high-risk" and to monitor the activities of such customers accordingly.

FBME recently has undergone independent third party audits, none of which has identified the "systemic failures in its AML controls" that the Notice asserts. Indeed, the contrary is true. In its most recent independent third party audit predating the FinCEN Notice, auditors determined that the Bank is "in principle in compliance" with Cypriot and EU standards. These independent audits identified certain areas for improvement, many of which FBME has either already implemented or for which FBME has documented project plans with milestone dates in place. In its Assessment, EY found that FBME's Compliance Program incorporates the requirements of the Directives, and that its Manual is in line with the requirements of the Directives. EY has identified certain

enhancements related to documentation, training, and other processes, and FBME is committed to further strengthening its Program in accordance with these recommendations. However, EY's recommended enhancements to the Program are far from "systemic failures in its AML controls."

FBME has a documented record of cooperation with regulatory and law enforcement authorities. Cypriot regulatory and law enforcement authorities, as well as financial institutions in other countries with which FBME maintains correspondent relationships, on many occasions have requested information from FBME pertaining to certain customers, accounts, or transactions. FBME has cooperated fully and provided the requested information in a timely manner. FBME would be pleased to provide documentary evidence of such cooperation.

4. *Notice Statement: "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." 79 Fed. Reg. 42639, 42640 (July 22, 2014)*

FBME does not facilitate the evasion of AML regulations; the Bank has never advertised its willingness to do so. FBME regularly monitors the internet for any inaccurate or misleading claims which might be made about the Bank. As discussed below in section II.A.5, FBME demands – in writing and, when appropriate, through outside counsel – that inaccurate statements be removed from websites, but there are legal limits to what the Bank can do to prevent misstatements by third parties. Thus, FBME cannot always ensure that the false statements are removed.

Indeed, in contrast to the statement in the Notice, FBME has a reputation among prospective clients and third party introducers for being particularly stringent relative to other banks both in Europe and particularly in Cyprus in its on-boarding of new customers and processing of payments. The Bank routinely receives complaint letters from customers and third party introducers bemoaning the stringent guidelines to which FBME adheres and its unwillingness to expedite account openings. FBME also works to the best of its ability to ensure that contrary messages are not advanced in any forum.

The Bank primarily markets itself to third party introducers at professional conferences and relies upon personal introductions through existing relationships. As part of its "Business Introducer Agreement" with third party introducers, FBME insists that such introducers obtain the Bank's prior written approval before using its name in any materials. The Bank enforces this rule and sends third party introducers letters demanding the removal of any unapproved advertising, regardless of the content.

FBME does limited advertising to the general public, such as posting signage at Larnaca airport in Cyprus and through its extensive local Corporate Social Responsibility program. FBME's promotional materials do not advertise the Bank's ease of use or evasion of regulations. Marketing materials primarily emphasize benefits related to the Bank's extensive international banking experience, and highlight its international network of correspondent banks, multi-lingual personnel, expanded working hours for different global markets, and geographically diverse client base. Besides its focus on international accessibility, FBME's promotional materials also emphasize a strong customer focus with individualized attention, a history of high liquidity, cutting-edge services, confidentiality, collaboration, and the benefits of a Cypriot presence, such as low corporate tax rates,

an EU regulated banking environment, and its strategic geographic location between Europe, Asia, the Middle East, and Africa.

5. *Notice Statement: "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.'" 79 Fed. Reg. 42639, 42640 (July 22, 2014)*

The Notice accurately quotes this misstatement by an unauthorized third party on a website unaffiliated with FBME. But the Notice fails to acknowledge that in January 2008, FBME identified this false statement and took action on multiple occasions to eliminate it. In fact, as explained in detail below, FBME has a documented record of opposing these sorts of misstatements because of the damage they do to the Bank's reputation.

Although FBME cannot control all the misstatements of others, it consistently seeks the removal of any false, maligning statements about the Bank that third parties publish on the internet. The Bank regularly searches the internet for references to FBME and sends letters requesting the removal of false statements to the parties who make or maintain them. Some examples of the Bank's efforts in this regard are as follows:

- With respect to the statement quoted in the Notice, FBME identified this statement in January 2008 and sent a letter to the website host on January 31, 2008, requesting the reference to FBME be removed. FBME's letter provided, "The statement regarding 'FBME Bank of Cyprus' is not accurate and since our name is mentioned in the article we are asking you to remove the reference to our name. Moreover, it is particularly harmful to FBME because FBME is being portrayed on this website as an institution participating in a gambling activity." The website making this statement, www.blackjackforumonline.com/Complete_Guide_to_Offshore_Bank_Accounts.htm, is unaffiliated with FBME. It is worth noting that FBME was not the only bank attacked in the statement. Identical allegations were made against five other banks alongside FBME.

- On January 31, 2008, FBME sent a letter to GoDaddy.com, the company that hosts blackjackforumonline.com, and similarly requested the removal of the false and defamatory statements on this website.

- On January 31, 2008, FBME sent a nearly identical letter to Domains by Proxy Inc. regarding its website. Despite FBME's efforts, the statement about FBME was never edited or removed.

- In 2010 and 2011, FBME sent several similar letters to the owners of a website entitled searchnfindarticles.com regarding false and defamatory statements about FBME involvement in gambling activity.

- On August 3, 2012, FBME sent letters to two UK companies (a website and a website host company) requesting the removal of an article referencing FBME on the grounds that it was "inaccurate, misleading, and posted without [FBME's] authority" from www.armadaboard.com.

- In October 2012, FBME's external counsel in the UK sent a Letter of Claim to the owner of the website www.cityclub-casino.com, Imperial e-club Limited in Antigua, its service provider, Paragon Internet Inc. in Canada, and its host, WebFusion Internet Solutions in the UK, threatening legal action if false statements instructing customers to wire money to an FBME account were not removed. The fund transfer related to the commencement of online gambling, and the stated recipient of the funds had not been an FBME accountholder since 2004.

- In October 2013, FBME sent letters to two Russian companies (a website and a website host company) demanding removal of false and defamatory statements from http://bankir.ru.

- On May 27, 2014, FBME sent a letter to GoDaddy.com regarding an unauthorized advertisement of a card purportedly owned by FBME.

- On June 11, 2014, FBME sent letters to two UK companies (a website and a website host company) demanding removal of defamatory statements from the website www.cypriot.org.uk.

Whenever FBME uncovers inaccurate or potentially defamatory information about it on third party websites, the Bank sends letters requesting that the entity remove the false information. In many cases, these letters have resulted in removal of the inaccurate mention of FBME from the website. If the websites do not remove the inaccurate information, FBME considers its options on a case-by-case basis. FBME regularly works with internal and external legal counsel with regards to these situations and has obtained legal opinions to aid in these decisions. In certain instances, FBME has pursued the matters in courts (both in Cyprus and abroad); however, the Bank often faces limitations to its ability to require the removal of these statements.

6. *Notice Statement: "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." 79 Fed. Reg. 42639 (July 22, 2014)*

FBME did not knowingly facilitate this transfer. To the contrary, in May 2009 FBME identified the relevant transactions as suspicious and made appropriate inquiries, consistent with its KYC policy, to understand the nature and purpose of the transfer, the relationship of the parties, and the business activities of the remitters. The client provided information sufficient to establish the apparent legitimacy of the transactions.

However, in July 2010, FBME received notification from another bank that a July 2010 transfer to the same client was fraudulent. Upon receiving this notice, FBME immediately froze the account. FBME conducted an investigation and concluded that the client may have been involved in fraudulent activities. Accordingly, FBME filed an STR on the transfer with MOKAS, and it kept the account frozen. In 2014, FBME delivered the frozen funds to the victim's lawyer's account in compliance with a court order. FBME has been required by law to maintain the account, keeping the remaining funds frozen due to pending litigation. At the conclusion of the litigation, FBME will disburse the funds in compliance with any court order that may be issued and close the account.

FBME has not willingly or knowingly associated itself with criminals or permitted known criminals to open accounts with FBME. In fact, the Bank has in place a Fraud Task Force Group ("FTG"),

consisting of the Group Head of Compliance, Group Head of Audit, Legal Counsel, Group Head of Operations, Head of Customer Services and Business Development, and Head of Risk. The FTG is focused on fraud perpetrated against the Bank and also receives updates about cases relating to fraud against Bank customers. The FTG educates all Bank departments about fraud risk indicators, as well as raises general awareness of potential fraud. The Bank is confident that its policies and procedures in place today permit the Bank to monitor customer activities in such a way as to detect illicit behavior.

B. Other Specific Statements regarding FBME

The Notice contains a number of other statements regarding specific transactions involving FBME. FBME in certain cases cannot respond directly to the cited examples without more specific information from the Treasury Department. However, the Bank would be pleased to provide any additional information and assistance possible to U.S., Cypriot and Tanzanian officials in their investigations of criminal activity and enforcement of related laws.

C. Additional Section 311 factors

According to Section 311 of the USA PATRIOT Act, the U.S. Government should consider, among other factors, the impact of the imposition of the fifth special measure upon the legitimate business activities of FBME. In its discussion of this factor, FinCEN notes that the "[l]egitimate activity at FBME's Cyprus branch is difficult to assess." FBME believes that a full assessment of its Compliance Program demonstrates that FBME's Cyprus branch is a legitimate member of the international banking community. Furthermore, the statements relied on by FinCEN in the Notice, including that FBME has a limited number of customers in Cyprus, that the Bank holds 90% of its assets in Cyprus or even that the Bank has a significant number of holding companies as customers in no way establish that the vast majority of FBME's customers do not use the Bank for legitimate business purposes.

FBME respectfully requests that the U.S. Government consider that FBME supports its customers' legitimate business activities and that the imposition of the fifth special measure will have a significant impact on the legitimate business activities of those customers and FBME itself. FBME's almost 10,000 customers make legitimate use of the Bank's services every day. And FBME's approximately 375 employees work hard to serve those customers in a reliable, compliant manner.

III. CONCLUSION

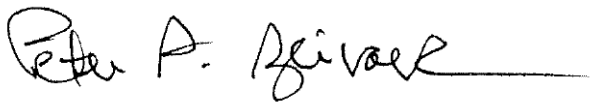
FBME has sought to demonstrate in this public comment its strong commitment to compliance, its firm opposition to the use of the Bank for illicit purposes, and its unequivocal resolve to work in cooperation with its regulators and with FinCEN to prevent financial crime whenever and wherever possible. As demonstrated by the reviews of independent third parties, the Bank has substantially strengthened its Compliance Program over recent years, and it has implemented a Program that is in line with applicable regulatory requirements. FBME recognizes, however, that every compliance program – including its own – can be improved, and the Bank is entirely committed to continuing to enhance its Compliance Program to FinCEN's satisfaction. To this end, Hogan Lovells and EY are working with the Bank to implement all appropriate compliance enhancements. In light of all these facts, FBME respectfully requests that the Notice and NPRM be withdrawn.

We understand from representations made by Mr. May of your office that, upon conclusion of the comment period, FinCEN and the Treasury Department, in consultation with other agencies of the U.S. Government, will review all of the comments received. We also understand that we will

engage in exchanges of additional information and points of view with FinCEN. We look forward to cooperating with FinCEN in this regard, and we respectfully request that FinCEN work with all appropriate dispatch to assess FBME's Compliance Program and enhancement plans so that FBME and its customers can return to their legitimate business activities as soon as possible.

Thank you for your consideration of the foregoing.

Sincerely,



Peter Spivack
Beth Peters
Evans Rice
Hogan Lovells US LLP
Counsel to FBME Bank Ltd.

cc: FBME Bank Ltd.
Jeanne Archibald
Louise Lamb
Anthony Capobianco