



Anti-Fraud Policy

(Bank Secrecy Act and Anti-Money Laundering Policy)

March 18, 2016

Policy Information

Document Title:	Anti-Fraud (Bank Secrecy and Anti-Money Laundering) Policy
Document Owner:	Legal and Compliance
Bank-Level Approver:	Disclosure
Board-Level Approver:	Board of Directors (Audit Committee)
Review Frequency:	Annually
Initial Effective Date:	March 18, 2016
Last Review Date:	November 20, 2015
Next Review Date:	March 2017

CONTENTS

CONTENTS 2

1. INTRODUCTION 3

1.1. Scope3

1.2. Related Documents4

1.3. Roles/Responsibilities4

1.4. Exceptions4

1.5. Violations4

2. POLICY 4

2.1. Money Laundering And Terrorist Financing4

2.2. AML Officer Designation And Duties5

2.3. Implementation Of Policy6

2.4. Reporting And Investigation7

2.5. Monitoring For Suspicious Activity And Fraud10

2.6. Money Laundering Risk Assessment11

2.7. OFAC Compliance12

2.8. Confidentiality And Recordkeeping12

2.9. Training Programs13

2.10. Independent Audit Of Aml Program13

2.11. Finance Agency Financial Instrument Fraud Reporting14

2.12. USA Patriot Act Sections 314(A) And 314(B)14

2.13. Suspended Counterparty Program14

2.14. Whistle-Blower Protection15

3. AMENDMENTS 15

4. APPROVAL AND REVIEW CYCLE 15

5. RELEVANT AUTHORITIES AND REFERENCES 15

6. DOCUMENT CHANGE RECORD 16

1. INTRODUCTION

The Federal Home Loan Bank of Indianapolis (Bank) is committed to a comprehensive anti-money laundering (AML) program for all of its business lines. It is the policy of the Bank to comply fully and completely with all applicable governmental requirements that have been designed to prohibit and prevent both actual and potential money laundering, as well as other activities that facilitate money laundering, and the funding of terrorists and/or other criminal activity.

This Anti-Fraud Policy (Policy), which is the Bank's Bank Secrecy Act (BSA), AML, and anti-fraud policy, will be reviewed at least annually and updated from time to time as necessary in response to changes in applicable law and changes in the Bank's operations.

This Policy applies to all Bank products, services, and investments, including, without limitation, Advances, collateral, MBS investments, unsecured investments, Acquired Member Asset programs, derivatives, Community Investment Program, Correspondent Services, Bank administration, and Office of Finance funding.

The Bank, acting through the Disclosure Committee is authorized to adopt, amend, and maintain procedures (Procedures) to implement this Policy. The Procedures may exclude other matters from the scope of this Policy.

In case of a conflict among the requirements of this Policy, the Procedures, applicable law, or regulation (including, without limitation, applicable guidance, advisory bulletin, Q&A, or other written advice of the Federal Housing Finance Agency), the following will govern in order of priority: (1) applicable law, (2) applicable regulation (as defined above), (3) this Policy, (4) the Procedures.

1.1. SCOPE

This Policy addresses:

- Money Laundering and Terrorist Financing
- AML Officer Designation and Duties
- Implementation of Policy
- Reporting and Investigation
- Monitoring for Suspicious Activity and Fraud
- Money Laundering Risk Assessment
- OFAC Compliance
- Confidentiality and Recordkeeping
- Training Programs
- Independent Audit of AML Program
- Finance Agency Financial Instrument Fraud Reporting
- USA Patriot Act
- Suspended Counterparty Program
- Whistle-Blower Protection

1.2. RELATED DOCUMENTS

Code of Conduct, Disclosure Policy, Whistle-Blower Policy, Finance Agency regulations, FinCen regulations and guidance, SEC rules and regulations.

1.3. ROLES/RESPONSIBILITIES

Table 1. Policy Name Roles and Responsibilities

Compliance, AML Officer	Responsible for all required reporting including SAR filings, OFAC compliance, Suspended Counterparty Reporting, as well as training and assessments of compliance
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.4. EXCEPTIONS

None.

1.5. VIOLATIONS

Willful or grossly negligent noncompliance with this Policy may subject a person to discipline per the Code of Conduct.

2. POLICY

All directors, officers and employees shall operate within the framework of this Policy, and other related Bank policies and procedures.

2.1. MONEY LAUNDERING AND TERRORIST FINANCING

2.1.1. Money Laundering. “Money laundering” is generally defined as engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or origins or otherwise constitute legitimate assets. Generally, money laundering occurs in three stages:

2.1.2. Stage 1 - Placement: Cash generated from criminal activities is “placed” in the financial system or the retail economy, often by converting the cash into monetary instruments, such as money orders or securities or investing it in real estate, commodities, or high-end consumer products (e.g., automobiles, boats, jewelry). Illegally obtained money is most vulnerable during the “placement” stage, because, over the years, regulators and law enforcement authorities have imposed a variety of reporting requirements and have required financial institutions, including Federal Home Loan Banks, to train their employees to look for suspicious transactions. To disguise the placement of unlawful funds, money launderers will often use a technique called “Structuring.” Structuring involves the breaking up of a transaction that would normally have to be recorded or reported into smaller transactions at dollar amounts below the recording/reporting thresholds.

2.1.3. Stage 2 - Layering: Funds are transferred or moved into other financial institutions to further separate the money from its criminal origin.

2.1.4. Stage 3 - Integration: Funds are reintroduced into the financial system and then integrated into the economy by purchasing legitimate assets or funding legitimate businesses or other criminal activities.

2.1.5. Terrorist Financing. Unlike money laundering, terrorist financing is typically motivated by ideological, rather than profit-seeking concerns, and often may not involve the proceeds of criminal conduct. Money laundering is frequently an important component of terrorist financing, and the methods used are often similar or identical to those used by money launderers. Large sums are not necessarily involved, and the original funds may well be legitimate rather than illegally obtained. One goal of terrorist financing is to establish flexible and mobile sources of funding for the purchase of products and services that will be used to further or commit terrorist acts.

2.2. AML OFFICER DESIGNATION AND DUTIES

2.2.1. Designation of AML Officer. As required under the BSA, the USA PATRIOT Act, and the Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing Government Sponsored Enterprises adopted by Financial Crimes Enforcement Network (FinCEN), the Bank hereby designates an AML Officer for the Bank (AML Officer). The AML Officer is responsible for: (1) overseeing the Bank's ongoing compliance efforts with respect to all state and federal AML laws, including monitoring compliance by the Bank's employees with their obligations under the Bank's AML program; (2) ensuring that the Bank's AML Program is updated as necessary; and (3) ensuring that all employees receive training on AML requirements and the requirements of this Policy before conducting business on behalf of the Bank and, thereafter, on an ongoing basis as needed. The AML Officer may also serve as the Bank's Financial Instrument Fraud Officer (FIFO) under the Federal Housing Finance Agency (Finance Agency) fraud reporting regulations, as the same may be updated, amended, and supplemented from time to time. Where different people are designated as AML Officer and FIFO, the Bank may distinguish their relative duties in procedures that are adopted from time to time.

The Board hereby designates the Compliance Director of the Bank as the AML Officer and the Deputy General Counsel as the Financial Instrument Fraud Officer. The AML Officer and the FIFO may delegate such responsibilities as he or she deems appropriate or desirable to effectuate the purposes of this Policy. Unless the context otherwise requires, references to the AML Officer herein will be deemed to include the AML Officer, the FIFO, and his or her respective identified designees.

2.2.2. AML Officer Duties and Responsibilities. The duties and responsibilities of the AML Officer include, but are not limited to, the following:

2.2.2.1. Maintain a thorough knowledge of all state and federal statutes pertaining to anti-money laundering with respect to the Bank's operations, including Office of

Foreign Assets Control of the U.S. Treasury (OFAC) requirements, detecting and addressing Red Flags¹ and Suspicious Activity Report (SAR) requirements.

- 2.2.2.2. Supervise the development and periodic updating of policies and procedures related to compliance with applicable federal and state statutes regarding anti-money laundering and related requirements.
- 2.2.2.3. Schedule and coordinate annual employee training sessions regarding applicable state and federal anti-money laundering and related requirements to ensure compliance therewith.
- 2.2.2.4. Supervise the proper completion, timely submission, and complete and accurate recordkeeping with respect to government filings pertaining to anti-money laundering and related requirements, including but not limited to SARs.²
- 2.2.2.5. Serve as liaison with law enforcement and regulatory agencies regarding matters of compliance/examinations/reports pertaining to anti-money laundering and related requirements.
- 2.2.2.6. Supervise the monitoring of statutory examinations conducted by any government agency pertaining to anti-money laundering and related requirements.
- 2.2.2.7. Supervise the maintenance of records related to any documents requested by law enforcement and/or regulatory agencies pursuant to subpoena, summons, or other administrative or court documents pertaining to anti-money laundering or related requirements.
- 2.2.2.8. Coordinate periodic independent audits of the Bank's AML program to effectuate Section 11 hereof.

2.3. IMPLEMENTATION OF POLICY

The Bank uses a combination of entity level controls, process level controls, and the diligence of individual Bank employees to prevent and detect actual and potential money laundering and fraud.

- 2.3.1 Entity Level Controls. The Bank maintains, and will continue to maintain, appropriate entity level controls reasonably designed to prevent and detect money laundering and fraud. These controls include, among other things: (1) this Policy, (2) fraud and other controls documented pursuant to Bank policies, procedures, and programs; and (3) other

¹ See Section 6.1 below.

² 31 C.F.R. § 1030.330 requires the filing of Currency Transaction Reports (CTRs). Because the Bank does not conduct retail banking and only engages in currency transactions with its insured depository institution members, and because currency transactions with such entities are exempt from CTR reporting, the Bank will not have cause to file CTRs. See 31 C.F.R. § 1010.315 (exempting currency transaction reporting with commercial banks). Should these facts or regulatory requirements change, the AML Officer will promptly review the Bank's CTR filing obligations to determine whether such filings may be required.

board and management approved policies that contribute to the Bank's money laundering and fraud prevention and detection efforts.³

- 2.3.2 Process Level Controls. For all financial transactions involving the Bank,⁴ the responsible Bank department(s) will maintain adequate and efficient process level controls reasonably designed to prevent and detect money laundering and fraud. These controls include, among other things, process-level fraud controls documented pursuant to Bank policies and procedures. Examples of different types of preventative or detective process level controls include Red Flags, authority limits, analyses, reconciliations, and independent reviews. Each department should also maintain an effective segregation of duties in accordance with Bank guidelines.
- 2.3.3 Responsibilities of Individual Employees, Officers, Directors, and Affordable Housing Advisory Council Members. In the course of fulfilling their duties to the Bank, all Bank employees, officers, directors, and Affordable Housing Advisory Council (Advisory Council) Members will exercise reasonable diligence to prevent, detect, and report money laundering and fraud.

2.4. REPORTING AND INVESTIGATION

- 2.4.1. Reporting Duties of All Bank Personnel. All employees, officers, directors, and Advisory Council members of the Bank will immediately report any known or suspected money laundering, suspicious activities, possible fraud, terrorist financing, Red Flags, and violations of this Policy. All such reports will be treated as confidential to the extent possible, and the Bank's Whistleblower Protection Policy will apply.
- 2.4.2. To Whom Reports Will be Made. Any employee or other person who makes a report under Section 5.1 will immediately notify his or her supervisor, the AML Officer or the FIFO. If not an employee, reports should be made to the AML Officer or the Chief Internal Audit Officer.⁵
- 2.4.2.1. Any supervisor or other manager who receives a report under Section 5.1 will notify the AML Officer.⁶
- 2.4.2.2. All reporting may be done confidentially through EthicsPoint at: 1-866-850-1408 or www.ethicspoint.com.

³ This Policy is not intended to alter ownership of or responsibilities under these other policies.

⁴ In addition to direct financial transactions, "financial transactions involving the Bank" also includes, without limitation: (1) the origination and pledge of advances collateral, (2) sales of mortgage loans into the Bank's Acquired Member Asset programs, and (3) the Bank's affordable housing program and other community investment activities.

⁵ The Ethics Officers are identified on the Staff Policy Portal and on the Bank's public website under "Contacts."

⁶ In addition, Section 12 – F of the Code of Conduct provides that officers, employees and directors of the Bank, as well as members of the Bank's Advisory Council, will also report fraud or possible fraud to the Chief Information Security Officer (and an Ethics Officer) if the matter involves a possible security breach with respect to the loss of a portable storage device containing Personal Information (as defined in the Code of Conduct).

- 2.4.2.3. Reports may be provided to senior officers or Directors, but should not be discussed with or reported to non-supervisory level employees at any time.
- 2.4.2.4. If a person making a report has reason to suspect that the recipient of the report might be involved in the activity identified in the report, they should report to a different person designated in Section 5.2. For example, if the person making the report suspects the AML Officer may be involved in the activity identified in the report, he or she should report to the General Counsel – Chief Compliance Officer, Deputy General Counsel, or the Chief Internal Audit Officer.
- 2.4.3. Investigations. An objective and impartial investigation, as deemed necessary, will be conducted as to any reports made under this Policy, regardless of the position, title, length of service, or relationship with the Bank of any party who might be or becomes involved in or becomes or is the subject of a report hereunder. The scope and extent of the investigation should be commensurate with the gravity of the report, and might include gathering additional information internally or from third-party sources. If in the course of investigating any complaint, the AML Officer determines that the Bank is required to file a SAR, then: (1) the AML Officer will prepare and file the SAR by the FinCEN filing deadline, and (2) the date of such determination will constitute the date of initial detection for purposes of compliance with Section 1030.320(b)(3) of FinCEN regulations, consistent with FinCEN guidance.⁷
- 2.4.3.1. AML Officer Directs Investigations. The AML Officer, in consultation with the appropriate management team, has the primary responsibility for overseeing the investigation of all reports made under this Policy, consistent with the requirements of applicable law, regulation, and regulatory guidance. The Bank will make every effort to keep the investigation confidential; however, from time to time outside experts such as legal counsel or auditors may be consulted in conjunction with the investigation. Also, the AML Officer will involve others from Human Resources, Legal, Internal Audit, Enterprise Risk Management (ERM), or other management as deemed appropriate. Where the report involves allegations of possible internal misconduct or may require the Bank to file an Immediate Notification under the Advisory Bulletin AB 2015-01, FHLBank Fraud Reporting, as the same may be updated, amended, modified, or superseded from time to time (Advisory Bulletin), the AML Officer will consult with the Chief Internal Audit Officer.
- 2.4.3.2. Advisory Notice. The President-CEO (CEO) and the Senior Vice President-Chief Financial Officer (CFO), will be apprised of the existence of any internal investigation, unless their potential involvement has been raised in any allegation or report leading to the investigation. They will also be kept apprised of the status of the investigation at least quarterly and prior to the end of any reporting period for which the CEO and CFO must provide written certifications and representations to the outside auditors, the Finance Agency or the Securities & Exchange Commission.

⁷ See FinCEN, *Suspicious Activity Reporting-Overview*, text at n.68, available at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm.

- 2.4.3.3. Chair of the Audit Committee and Investigations. After an initial review and a determination that the suspected activity is internal to the Bank, may require the Bank to file an Immediate Notification, or otherwise is material and warrants additional investigation, the Chief Internal Audit Officer and the AML Officer will notify the Audit Committee and management, as appropriate. The Chair of the Audit Committee may determine that the Chief Internal Audit Officer or the AML Officer may initiate an internal investigation. The Chair of the Audit Committee, or the Vice Chair if the Chair is precluded from acting under this policy, will determine the appropriate investigative course of action and will keep the Audit Committee so advised. The Audit Committee will keep the Board apprised, and the Audit Committee or the Board may elect to form a special committee to investigate or review and act upon the findings of any internal investigation. The Chair of the Audit Committee may require an independent investigation of the circumstances by outside counsel or other external consultation. The Board or Audit Committee may engage its own experts or consultants as it deems appropriate. Upon conclusion of any internal investigation, the results will be reported to the appropriate management representatives and the entire Audit Committee. In addition, updates of any investigations or findings of fraud will be provided to the Audit Committee as requested by the Chair of the Audit Committee.
- 2.4.3.4. Unauthorized Investigations Prohibited. Unauthorized Bank staff may not, on their own initiative, investigate any matter addressed by this Policy.
- 2.4.4. Filing SARs. The Bank will file a SAR for any activity conducted or attempted through the Bank involving (individually or in the aggregate) \$5,000 or more where the Bank suspects, or has reason to suspect, that:
- 2.4.4.1. the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
 - 2.4.4.2. the transaction is designed, whether through structuring or otherwise, to evade the requirements of the BSA regulations;
 - 2.4.4.3. the transaction has no apparent business or lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and, after examining the background, possible purpose of the transaction, and other facts, the Bank has found no reasonable explanation for the transaction; or
 - 2.4.4.4. the transaction involves the use of the Bank to facilitate criminal activity.

The Bank will file a SAR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. The AML Officer will file all required SARs using FinCEN's BSA E-Filing System, available at <http://bsaefiling.fincen.treas.gov/main.html>, or such other method(s) that FinCEN may order.

2.4.5.AML Officer Responsible for Filing SARs. The AML Officer will be responsible to ensure that any SARs are filed as required. SARs must be filed no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, the AML Officer may delay filing the SAR for up to an additional 30 calendar days, or a total of 60 days after the date of initial detection of the facts, pending identification of a suspect. Among the information the AML Officer will use to determine whether to file a SAR are exception reports that include transaction size, location, type, number, and nature of the activity. The AML Officer will not base his or her decision on whether to file a SAR solely on whether the transaction falls above a set threshold. In high-risk situations, the AML Officer will notify law enforcement immediately and will file a SAR with FinCEN. In addition to the reports required hereunder, the Bank may, in its discretion and under the direction of the AML Officer, file a SAR for any suspicious transaction that the AML Officer believes is relevant to the possible violation of any law or regulation, but whose reporting is not otherwise required by FinCEN or the Finance Agency.

2.4.6.Notification of Executive Management and the Board. The AML Officer will provide a summary report on all Bank SAR filing activity to the Audit Committee on a quarterly basis. For any SAR that the AML Officer, in consultation with the Bank's CRM, determines involves a significant financial or reputational impact on the Bank, the AML Officer will immediately notify the Executive Management Committee (EMC). The EMC will determine whether to notify the Chairs of both the Board of Directors and the Audit Committee.

2.4.7.Personnel Actions Pending Investigations. During any investigation hereunder, and depending on the circumstances, the Bank may suspend employees who are the subject of the investigation with pay. If the investigation substantiates any suspicious activity, fraud, money laundering, or terrorist financing, management may take appropriate disciplinary action, up to and including termination, in consultation with legal counsel, in addition to pursuing any legal remedies which may be available. If an allegation of any suspicious activity, fraud, money laundering, or terrorist financing by a Director or Advisory Council member is substantiated, management will take all steps necessary to remove such person from his or her position, in addition to all legal remedies that may be available.

2.5. MONITORING FOR SUSPICIOUS ACTIVITY AND FRAUD

2.5.1.Monitoring for Money Laundering, Suspicious Activities, and Fraud. The Bank will monitor a sufficient amount of activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "Red Flags" identified in relevant lists. Each of the Bank's departments will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the AML Officer so they may be reviewed and, when necessary, reported to the appropriate authorities.

2.5.2.Detecting Red Flags. Red Flags can arise at any time. An individual Red Flag can be business- or industry-specific or can apply more broadly to all businesses and industries in which our customers are active. Management will develop one or more Red Flag lists and train appropriate Bank personnel on such warning signs.

2.5.3. Responding to Red Flags. When an employee of the Bank detects any Red Flag, he or she will be responsible for immediately reporting the Red Flag in accordance with Section 5.1.

2.5.4. Customer Due Diligence. The Bank's customers are its members, housing associates, and former members with whom the Bank still has transactions. These customers are generally subject to the BSA, USA PATRIOT Act, and AML obligations. The Bank may require, through appropriate policies, that customers agree to maintain AML controls effective to prevent the use of the Bank's products and services to facilitate money laundering, terrorist financing, fraud, or other illicit activity. If, in the course of the Bank's oversight and monitoring of customers' financial condition and Bank transactions, information comes to the attention of the Bank personnel that indicates that any customer fails to have AML controls effective to prevent the use of the Bank's products and services to facilitate money laundering, terrorist financing, fraud, or other illicit activity, such personnel will promptly report such facts to the AML Officer. Based on such reports and other information available to the Bank, the AML Officer may make a recommendation to the Member Services Committee to adopt heightened controls with respect to such customer to mitigate the potentially higher AML risk associated with the customer.

2.5.5. Reliance on Third Parties. Prior to engaging the services of the third party to perform AML duties, the Bank will perform due diligence on the third party in compliance with the Vendor Management and Procurement Policy. The Bank may adopt procedures to rely on the performance of another financial institution or other third party for certain elements of the Bank's AML program, consistent with Section 326 of the USA Patriot Act and the regulations promulgated thereunder. The Bank also will require that service providers report any Red Flags to the AML Officer.

2.6. MONEY LAUNDERING RISK ASSESSMENT

The development and implementation of the Bank's AML program must be based on an effective risk assessment process. For this reason, the Bank is required to conduct formal AML/OFAC risk assessments of its business, customers, products and services, and geographic locations and markets.

The AML Officer will determine inherent money laundering risks, then review mitigating controls, and in consideration of the inherent risks and mitigating controls, determine the overall residual money laundering risk. The AML Officer will also consider the mitigating controls maintained by the Bank pursuant hereto or otherwise. The results of the Risk Assessment will be reported to the Risk Committee and the Audit Committee.

The Bank's money laundering risk assessments must be updated annually, unless more frequent risk assessments are required by applicable AML laws. The Bank's money laundering risk assessment must also be updated before the Bank engages in any "new business activity" as defined in Section 1272.1 of the Finance Agency's regulations to reflect the new or materially changed product or service being offered.

2.7. OFAC COMPLIANCE

2.7.1. OFAC Checks Required. The Bank will comply with OFAC regulations, which prohibit transactions involving certain individuals, entities, or countries that are subject to sanctions or other special concerns. Before engaging in certain designated kinds of transactions, the employee initiating such action will check to ensure that a customer does not appear on the United States Department of the Treasury's OFAC Specifically Designated Nationals and Blocked Persons List and is not from, or engaging in transactions with people or entities from countries and regions subject to economic sanctions or embargo. The AML Officer will designate the classes of transactions that require an OFAC check before they may be performed, and the reporting processes to be undertaken in the event of a match, which will include, at minimum, wire transactions, letter of credit trustees and beneficiaries, employees at time of hire, and quarterly reviews of financial counterparties. If there is no potential match with the OFAC lists, the transaction or activity may proceed. OFAC risk will be assessed in the Bank's money laundering risk assessment.

2.7.2. Coordination with SAR Reporting. As part of the Bank's SAR filing process, any blocking reports or rejected transaction forms sent to OFAC will be reviewed to determine whether anything contained therein constitutes suspicious activity under FinCEN and Finance Agency regulations.

2.8. CONFIDENTIALITY AND RECORDKEEPING

2.8.1. SAR Confidentiality. The Bank will maintain as **strictly confidential** any SAR or other report required by the Finance Agency, and any such report's supporting documentation. **NO Bank personnel will notify any person involved in the transaction that the transaction has been reported or that the transaction is under investigation.** In general, disclosure of the fact that a SAR filing is contemplated or has been made is a violation of federal law. Any Bank employee who is subpoenaed or required to disclose a SAR or other report required by the Finance Agency, or the information contained in such report will report the existence of that subpoena or requirement immediately to the AML Officer, and prior to disclosure of the SAR or other report required by the Finance Agency, or the information contained in such report. Except where disclosure is requested by FinCEN or other appropriate law enforcement or regulatory authority, as determined by the AML Officer in consultation with the Legal department, the Bank will decline to produce the SAR or other report required by the Finance Agency, or any information that would disclose that a SAR or other report required by the Finance Agency was prepared or filed. None of our directors, officers, employees, contractors or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information the Bank used to respond to it.

2.8.2. Maintaining SARs, Finance Agency Filings, and Other Records. Every SAR or other report required by the Finance Agency, and copies of any supporting documentation referenced therein, will be maintained separately from all other books and records of the Bank in a secure location to avoid inadvertent disclosure of SAR or other report required by the Finance Agency, limiting access to the location where the records exist, and preventing any suspected individuals from having access to the records. The AML Officer and the Legal

department will handle all subpoenas or other requests for information related to SARs and other reports required by the Finance Agency. The Bank will also maintain records related to matches found in OFAC searches.

2.8.3. Holding Period. The AML Officer will retain copies of any SAR or other report required by the Finance Agency filed and any supporting documentation for at least 5 years from the date of filing. The AML Officer will make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state regulators, upon request.

2.9. TRAINING PROGRAMS

2.9.1. Training Required. The Policy is intended to be supplemented by training of all the Bank's directors, officers, Advisory Council members, and employees on at least an annual basis, and including new hires. The AML Officer will develop, coordinate, and/or provide ongoing employee training. Training may be in such format as the AML Officer may designate, as necessary to effectuate full compliance with AML laws and regulations and Bank policy. Training materials will be tailored to correspond with the employee's daily tasks. The training course offered may include how to identify Red Flags and signs of money laundering, what to do once the risk is identified, and the employee's role in the Bank's compliance efforts and how to perform that role, the Bank's record retention policy related to AML compliance, and consequences for non-compliance.

2.9.2. Training Records. The AML Officer will maintain records of which persons received training, the dates of training, and the subject matter of the training.

2.9.3. Tailored Training. From time to time, the AML Officer may determine that certain employees or departments require additional specialized training, and may provide specialized training or request such specialized training be undertaken.

2.10. INDEPENDENT AUDIT OF AML PROGRAM

2.10.1. Testing. Independent testing of our AML program will be performed by the Bank's Internal Audit department. Unless the Audit Committee determines otherwise, the Internal Audit department may choose an independent, qualified third-party auditor to perform the AML audit in its place.

2.10.2. Evaluation and Reporting. The independent testing will test compliance with this Policy; applicable sections of the BSA and the USA PATRIOT Act; and the SAR reporting requirements, and will include a review of how suspicious activity is monitored and identified, whether identified suspicious activity was reviewed and appropriately handled; and whether suspicious activity was properly reported.

2.10.3. Timing of Testing. AML testing will be performed on a schedule determined by the Audit Committee, and in no event less frequently than once every eighteen months. Upon and the AML Officer, and that report will be shared with the Bank's Risk Committee. The Bank will address and respond to each of the resulting recommendations in a timely manner.

2.11. FINANCE AGENCY FINANCIAL INSTRUMENT FRAUD REPORTING

It is the Bank's policy to comply with Part 1233 of the Finance Agency's regulations, *Reporting of Fraudulent Financial Instruments*, and the Advisory Bulletin. The Bank will also timely prepare and file all reports contemplated by Part 1233 and the Advisory Bulletin. Applicable requirements will be set forth in the Procedures.

2.12. USA PATRIOT ACT SECTIONS 314(a) AND 314(b)

Under Section 314 of the USA PATRIOT Act, the Department of the Treasury has issued regulations to encourage cooperation among financial institutions, financial regulators, and law enforcement officials for the purpose of sharing information regarding individuals, entities, and organizations "engaged in or reasonably suspected, based on credible evidence, of engaging in" terrorist acts or money-laundering activities. Specifically, the information sharing provisions address the following two types of information sharing.

- 2.12.1. Record Search – Section 314(a). The Bank will adopt procedures to implement applicable obligations under Section 314(a) of the USA PATRIOT Act.
- 2.12.2. Voluntary Information – Section 314(b). Section 314(b) of the USA Patriot Act allows for financial institutions to share certain information with regard to money laundering and terrorist financing issues among themselves for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities. The AML Officer may (but is not required to) register and certify on behalf of the Bank with FinCEN under the Section 314(b) program.

2.13. SUSPENDED COUNTERPARTY PROGRAM

2.13.1. Compliance Required. It is the Bank's policy to comply with the Finance Agency's suspended counterparty program (SCP Program) requirements. As used in this section, "Counterparty" means an individual or entity with which the Bank has, or in the past three (3) years has had, a contractual, financial, or business relationship. In the event that any Bank employee becomes aware that a Counterparty or an affiliate of a Counterparty either:

- 2.13.1.1. has, within the past three (3) years, been criminally convicted of fraud, embezzlement, theft, conversion, forgery, bribery, perjury, making false statements or claims, tax evasion, obstruction of justice, or any other similar offense, in each case in connection with a mortgage, mortgage business, mortgage securities or other lending product; or
- 2.13.1.2. was, within the past three (3) years, suspended or debarred by any Federal agency for conduct that would constitute an offense described above,

then such Bank employee must promptly report the matter to the AML Officer. The AML Officer will review the report; determine whether the matter must be reported to the Finance Agency

under the SCP Program; and, in consultation with the EMC, prepare and submit any required report to the Finance Agency.

2.13.2. Suspension Orders. The Bank will comply with any valid orders from the Finance Agency directing the Bank to cease conducting business with individuals and entities suspended by the Finance Agency pursuant to the SCP Program, to the extent mandated by SCP Program requirements. The AML Officer is responsible for notifying relevant Bank departments of any changes to the Finance Agency’s list of suspended counterparties.

2.14. WHISTLE-BLOWER PROTECTION

2.14.1. This Policy is subject to the Bank’s Whistle-blower Policy. However, this Policy will control in the event of any conflicts with the provisions of the Whistle-blower Policy. No employee or person acting on behalf of the Bank in attempting to comply Be dismissed or threatened with dismissal;

2.14.2. Be disciplined or suspended or threatened with discipline or suspension;

2.14.3. Be penalized or have any other retribution imposed; or

2.14.4. Be intimidated or coerced;

with this Policy will:

based upon the fact that the employee or other person has reported an incident or participated in an investigation in accordance with the requirements of this Policy. Violation of this section of the Policy will result in disciplinary action, up to and including dismissal. If an allegation is made in good faith, but is not confirmed by the investigation, no action will be taken against the originator. However, malicious allegations will result in disciplinary action against such individual.

3. AMENDMENTS

The Board may amend this Policy at any time.

4. APPROVAL AND REVIEW CYCLE

This Policy is effective as of March 17, 2016. The Audit Committee will review this Policy, recommend any changes, and recommend Board approval at least once per calendar year.

5. RELEVANT AUTHORITIES AND REFERENCES

FinCen requirements, Bank Secrecy Act, OFAC rules and regulations, FHFA regulations and Advisory Bulletins



6. DOCUMENT CHANGE RECORD

Version	Date	Description	Revised by

O:\sharing\Executive_Legal\POLICIES\Code of Conduct with Exhibits\2016 C of C revisions\Anti-Fraud Policy FINAL 3-16.docx