



Federal Reserve Bank of New York

**Compliance Manual of Procedures
Central Bank and International Account Services
- Account Control**

GRATED MAT

Table of Contents

| | |
|--|-----|
| Section 1: Introduction..... | 1 |
| Section 2: CBIAS Account Relationships | 6 |
| Section 3: Risk Based Approach and Restricted and Monitored Accounts | 9 |
| Section 4: OFAC and Exemption 7 | 16 |
| A. OFAC | |
| Exemption 7 | |
| C.List Management | |
| D. Transaction monitoring | |
| Section 5: Compliance Hold | 35 |
| Section 6: High Scrutiny Monitor | 38 |
| Section 7: Due Diligence | 42 |
| Appendix 1-A Exemption 7 Inputs and Flow..... | A-1 |
| Appendix A: Exemption 7 for Interacting with Exemption 7 | A-2 |
| Appendix B: Payments vs. Receipts | A-3 |
| Appendix C: Updating New OFAC List in Filter | A-4 |
| Appendix D: High Risk Typologies..... | A-5 |
| Appendix E: AML Red Flags | A-6 |

Section 1: Introduction to Account Control's AML/OFAC Compliance Operations

The Federal Reserve Bank of New York (FRBNY or Bank) offers accounts and provides financial services to Foreign and International Monetary Authorities, such as foreign central banks, foreign governments, and certain international organizations ("FIMA customers"). A full description of all the services the Bank provides to its FIMA customers is available on the Bank's FIMA customer website. The provision of accounts and services serves important Federal Reserve and U.S. Government objectives, but the accounts and activities entail financial, compliance and reputational risk to the Bank. As mandated by the Bank's Anti-Money Laundering Policy ("AML Policy"), to address these risks, the operating area of the Bank responsible for managing these accounts – the Central Bank and International Account Services area of the Markets Group (CBIAS) – has developed compliance procedures summarized in this Manual of Procedures ("MOP").

Account Control (AC) of CBIAS has developed this MOP to identify, assess, monitor, and report legal, regulatory, and reputational risk with the goal of meeting the following objectives:

- 1.) Comply with U.S. laws and regulations relating to Office of Foreign Assets Control ("OFAC");
- 2.) Apply principles of U.S. anti-money laundering regulations (principally the Bank Secrecy Act);
- 3.) Protect the Bank's reputation and avoid financial risks associated with the provision of financial services to FIMA customers.
- 4.) Ensure compliance with court orders and other legal process.
- 5.) Ensure compliance with Bank and Board of Governors of the Federal Reserve System ("BOG") regulations, policies, and procedures.
- 6.) Protect the interests of the Bank, including avoiding potential embarrassment, by proactively identifying and responding to potentially sensitive circumstances that could result in a legal claim and/or reputational risk.
- 7.) Protect the interests of the Bank's customers by guarding against improper use of a customer's account, and improper transfer of assets out of such accounts.
- 8.) Protect the interests of the Bank, the Federal Reserve System and the U.S. Government in their bilateral relations with other nations.

The regulations of the Department of the Treasury Office of Foreign Assets Control (OFAC) apply to FRBNY's operations and must be complied with by relevant business areas, including CBIAS. The Bank's OFAC Policy outlines the responsibilities of the business area for ensuring compliance. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals; additional information is provided in the Bank's OFAC policy. Additionally, AC's program to monitor account activity for OFAC violations is included in Section 4 of this MOP. As it relates to the Bank's compliance with anti-money laundering law, while FRBNY is not subject to many of the laws and regulations that mandate AML programs, such as the Bank Secrecy Act (BSA), it is FRBNY policy to adopt practices consistent with the spirit of these laws and regulations in practice.

The BSA and its amendments, including provisions of the USA PATRIOT Act of 2001, is the principal U.S. anti-money laundering law, intended to safeguard the U.S. financial system from the abuses of financial crime, including money laundering, terrorist financing and other illicit transactions that have damaging social and financial effects worldwide¹. Financial organizations develop compliance programs and controls in order to prevent and deter these activities and to protect themselves from risk. A full explanation of terrorist financing, the stages of money laundering, and the various legislation comprising the U.S. anti-money laundering regime are available in the Federal Financial Institutions Examination Council BSA/ Anti-Money Laundering Examination Manual,² as well as the Bank's AML Policy. The Bank's AML policy is available at: [Redacted] Exemption 7 Additional reference material on anti-money laundering and economic sanctions programs is provided at the end of this section.

The Bank's AML program designates a Chief Compliance Officer and assigns him the responsibility of, among other things, determining what constitutes suspicious activity, including reviewing specific instances of potentially suspicious activity and, with the advice of counsel, reporting it to the relevant authorities.

AML programs are risk-based, and the Bank's Compliance program has taken several steps to identify the customers, services and activities that present the highest risk to permit it to prioritize the review of high-risk transactions. [Redacted] Exemption 7

The principal responsibility for CBIAS' AML/OFAC compliance program resides in the Account Control Group (AC). AC coordinates with the Legal Group and the Compliance Function of the Bank to fulfill the objectives stated earlier. In particular, there are five core areas of responsibilities under the AML and OFAC Policies which include:

- (1) Identifying the AML and OFAC risks facing their business area and implement control activities designed to address those risks;
- (2) Conducting an appropriate level of transaction monitoring, and escalate unusual or atypical activity identified through monitoring efforts and in the normal course;³
- (3) Ensuring ongoing compliance with adopted AML/OFAC policies and procedures;
- (4) Ensuring that local staff receives appropriate AML/OFAC training; and

¹ The full list of statutes and regulations that make up the Bank Secrecy Act are available at http://www.fincen.gov/statutes_regs/bsa/.

² http://www.ffiec.gov/bsa_aml_infobase/default.htm

³ See Section 3: Risk Based Approach and Restricted and Monitored Accounts, Section 4: OFAC and [Redacted] Exemption 7 Section 5: Compliance Hold, Section 6: High Scrutiny Monitor, Section 7: Due Diligence.

- (5) Implementing specific recommendations made by Compliance with respect to any transaction, proposal, or issue, or raise the matter with the Group's Executive Vice President for further deliberation (See Section IV of the Bank's AML Policy).

Additionally, under the Bank's OFAC Policy, the responsibility of AC as the business area includes, "establishing OFAC procedures and controls that are in compliance with OFAC programs, and dedicating appropriate staff and budget resources to maintaining and implementing those procedures, including real-time or periodic screening of transactions, counterparties or account-holders, as applicable. Business areas are responsible for performing an initial investigation of potential OFAC violations in their area, and if necessary, escalating the matter to members of the [redacted] Exemption 7. The Compliance Function acts as the point of escalation for potential matches to OFAC's Specially Designated Nationals and Blocked Persons ("SDN") list while the Legal Function interprets OFAC regulations, investigates potential geography-based OFAC matches, and provides general guidance on OFAC-related issues. The Legal Function is also responsible for reporting blocked or rejected transactions or assets to OFAC in accordance with the Bank's legal obligation to do so under OFAC's regulations.

CBIAS' AC applies a risk-based approach to its compliance program by prioritizing its monitoring and analysis of higher-risk FIMA accounts and services through evaluation and utilization of [redacted] Exemption 7 and through its own assessments and determinations. AC compliance efforts consist of three main components: 1) real-time monitoring of all CBIAS transactions for OFAC regulations which is facilitated by interdiction software (described in MOP Section 4); 2) ex-ante monitoring of CBIAS accounts and services that pose the highest risk, which is termed "Compliance Hold" (described in MOP Section 5); and, 3.) ex-post monitoring of medium- and high-risk CBIAS accounts, which is detailed in AC's daily High Scrutiny Monitor (described in MOP Section 6). AC analysts conduct due diligence on transactions of concern highlighted in these three principal activities (described in MOP Section 7). Analysis of account activity and development of account profiles also supplement AC's compliance efforts.

While the primary responsibility for compliance in CBIAS resides in AC, all CBIAS staff are required to be aware of FRBNY compliance obligations. An on-line training program has been developed to facilitate understanding of this responsibility that all CBIAS staff are required to complete. The training outlines the CBIAS compliance program and provides an overview of sanctions program and AML and CTF principles and it is required that all CBIAS staff complete this training. Additionally, training on advanced topics in OFAC and AML are provided to AC compliance analysts so that they may become subject matter experts.

Key AML/OFAC Compliance References Utilized in AC Compliance Program

Financial Action Task Force

(<http://www.fatf-gafi.org/pages/>)

FATF is an inter-governmental body that sets global standards for anti-money laundering and counter terrorist financing (AML- CTF). The body's Forty Recommendations and Special Recommendations outline the critical components of an effective AML-CTF regime. Their

website includes a link to resources on international AML and CTF conventions and materials from the United Nations.

Financial Crimes Enforcement Network

(www.fincen.gov)

The U.S. financial intelligence unit that is responsible for administering the Bank Secrecy Act and receiving Suspicious Activity Reports from U.S. financial institutions. The website details all U.S. statutes and regulations on anti-money laundering.

Federal Financial Institutions Examination Council BSA/ Anti-Money InfoBase

(http://www.ffiec.gov/bsa_aml_infobase/default.htm)

An electronic source for training AML/BSA examiners that includes detailed information on components of a bank's compliance program.

Office of Foreign Assets Control

(<http://www.treas.gov/offices/enforcement/>)

The U.S. Department of the Treasury's OFAC is responsible for administering and enforcing economic and trade sanctions. Their website details U.S. sanctions programs as well as compliance guidance for the banking industry.

U.S. Department of the Treasury- Office of Terrorism and Financial Intelligence

(<http://www.treas.gov/offices/enforcement/>)

The Office of Terrorism and Financial Intelligence (TFI) marshals the department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats.

Wolfsberg Group

(<http://www.wolfsberg-principles.com/>)

The Wolfsberg Group is an association of eleven global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

Section 2: CBIAS Account Relationships

Introduction

The Federal Reserve Bank of New York as part of the Federal Reserve System maintains account relationships with other central banks, foreign governments and international financial organizations, and maintains these relationships on behalf of the system. Central Bank and International Account Services, within the Markets Group of the FRBNY, is responsible for maintaining these accounts at FRBNY. CBIAS currently maintains over 500 accounts for over 250 foreign and international monetary authorities. Because many of the world's foreign and international monetary authorities already hold accounts at the FRBNY, the establishment of an account relationship with a new customer is relatively infrequent.

The authority of FRBNY to establish accounts for 'foreign banks or bankers, or foreign states' is found in Section 14(e) of the Federal Reserve Act (FRA). The FRBNY policy on opening accounts is more restrictive, however, generally limiting CBIAS account holders to institutions with central banking responsibilities. The earliest accounts at the Bank were established for its central banking counterparts. The foreign customer base eventually expanded to include those institutions such as currency boards and governmental financial entities, that, while not strictly central banks, exercised central banking functions, particularly in the management of official foreign exchange reserves. Accounts have also been opened for international or regional institutions that have characteristics comparable to central banks. Pursuant to Regulation N, establishment of such accounts require approval of the BOG.

FRBNY also has authority to establish accounts by the directive of the U.S. Treasury as fiscal agent of the U.S. Government under Section 15 of the FRA, as well as accounts authorized by specific U.S. legislation pursuant to which FRBNY acts as fiscal agent to certain international financial organizations.

Exemption 7

Procedures for Establishing New Account Relationships: Regulation N Accounts

On receipt of a request from an institution to establish an account at the Federal Reserve Bank of New York, the typical process follows these steps (the order of steps may vary):

1. CBIAS management, in consultation with Legal and the Compliance Function, review the request and gather/refer to publicly available information, including

2. Based on this research, determine if the organization appears to generally meet the criteria for establishing an account at the Bank as a central bank or monetary authority, such as responsibility for:

- acting in the capacity of fiscal agent for a nation's government;
- currency issuance and/or control;
- the licensing and/or supervision of banks;
- the execution of exchange rate policies;
- the issuance of government securities;
- the operation and/or supervision of the payments system;
- establishing and executing monetary policy; and
- maintaining and managing foreign exchange reserves.

In the event that there are concerns about the country, organization or officials, then the review must be escalated to involve Markets, International Affairs, Legal and Compliance senior management, and may extend to the Federal Reserve Board. The Treasury or State Department may also be consulted (this is often done by the BOG).

3. If the institution, as defined in their request or based on research findings, appears to meet any or all of the above criteria, send an initial reply outlining the general criteria for establishing such a relationship, requesting further information about the functions and responsibilities of the institution, and requesting an official copy of the institution's establishing laws or statutes, in English translation. *In addition, request information about the general purpose of the account and the institution's intended use of the account.*
4. On receipt of the establishing documentation, forward a copy to the Legal Department and the Compliance Function with a request for review to determine eligibility to establish an account at the Bank. The Legal Department and Compliance Function will prepare a memo based on this review advising of, and explaining their recommendation in regard to, approval of the request.
5. If Legal concludes that the Bank has authority to establish an account under the FRA, then on receipt of a memo from Legal prepare a summary of their findings in an Aide Memoire that will be reviewed and approved by a CBIAS Officer.
6. Prepare, in consultations with Legal, a letter to the Head of International Finance at the BOG, for the signature of the CBIAS Senior Vice President, using the summarized information in the Aide Memoire.
7. On receipt of an approval letter from the BOG, prepare account documents and cover letter to the prospective FIMA customer advising of approval to establish an account and describing the account services. The letter will request a current copy of the organization's list of authorized signatories. The enclosed documents to be executed will include:
 - Account Agreement
 - Supplemental Account Agreement
 - Understanding with Regard to Authenticated Telecommunications
 - Draft Letter of Standing Instructions
8. If no issues are raised, the account is established on FRBNY's books.

This due diligence conducted on an organization at account opening is an important piece of AC's compliance efforts which helps mitigate risks involved in providing account services to its FIMA customers. It helps ensure the establishment of the account is for official nature. Additionally, the account opening procedures detailed above and the supporting documentation provide ARS and AC a better general understanding of the customer and the account's anticipated account activity, all of which provide the context necessary for monitoring transactions. Executed documents also help establish the customer's understanding of FRBNY account usage as well as persons authorized to instruct on the account. All information related to account opening is archived in individual customer files at [redacted] Exemption 7 and should be considered a key reference for AC compliance efforts.

Section 3: Risk Based Approach and Restricted and Monitored Accounts

Applying a Risk-Based Approach to CBIAS Compliance Efforts

As mandated by the Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Manual (“FFIEC Manual”), as well as FRBNY’s AML Policy, AC applies a risk-based approach to its compliance efforts in order to most effectively and efficiently deploy its resources. A risk-based approach distributes resources to the accounts and services that present the most compliance risk to the Bank. Greater scrutiny is applied to higher risk accounts and services. Accounts are classified in two monitoring categories, “Restricted” or “Monitored.”

Exemption 7



Exemption 7

Country Risk Rating Factor for Classification of Accounts

Because CBIAS' customer base is primarily comprised of foreign central banks, a useful tool for assessing AML risk in these accounts is through a risk matrix that evaluates individual country

Exemption 7

Additionally, monitoring news and current events is a critical component of AC compliance efforts as world events can have a bearing on account activity. Therefore, AC analysts should be aware of news generally, make connections to account activity, and be aware of any possible associated compliance risk.

Exemption 7

AC Management will then consult with Legal and Compliance Function to determine whether the type of monitoring on the account should change. Procedures that detail how account status is changed are outlined below.

Risk based approach to Services

Exemption 7

Internal FR

Exemption 7



Monitoring the Activity of High-Risk Accounts

Exemption 7



Exemption 7

Account Changes Related to Current Events

Exemption 7

AC has established Account Management Guidelines (“Guidelines”) that set forth the process that AC staff must adhere to when such situations arise. The Guidelines articulate the events that would trigger a change in a country and/or account status and the resulting coordination between Legal, the Compliance Function, and AC that must occur. When appropriate, Legal will be in communication with the U.S. Department of State in order to clarify current events and any changes that may affect the central bank and corresponding control of the FRBNY account. The Guidelines are available at [Exemption 7](#)

In such instances, AC should also consider the following to mitigate risk:

Exemption 7

As detailed below, pre-requisites for resuming normal operations may include some or all of the following:

- Receipt of a certification under Section 25(b) of the Federal Reserve Act from the U.S. Secretary of State designating a person or persons authorized to control the assets of the central bank (usually, the central bank governor) accompanied by a signature specimen of the authorized person(s); and

Exemption 7

In order to keep the “Restricted and Monitored” Account list up to date, AC will periodically review and make recommendations to add or remove a country from the list. Exemption 7

Following these periods AC staff can review the account and assess whether removal from Restricted status is warranted. This assessment is also made for accounts that have been placed on Restricted status as outlined in the Guidelines. Generally, an account will be reviewed for potential change in status when the event causing the change in status is resolved and normal account activity is observed. Exemption 7

If CBIAS believes the removal from Restricted status is due, the reasons will be included in an account review write-up⁷, which will then be forwarded to the Compliance Function (with copy to Legal) that will notify them of the change.

Checklist for Resumption of Relations with Account Holders or return to normal Monitored Status

The FRBNY may face the need to resume, or normalize, its relationship with the account holder once the conditions change that created the restrictions. While circumstances will vary based on the strategic importance of a particular country, it is advisable to consider consulting other groups of the Bank, in particular, Legal and Compliance Function.

In most cases involving issues of ownership and/or management of the account, the pre-requisite to FRBNY beginning normalizing an account relationship is a certification by the U.S. Secretary of State, designating individual(s) authorized to control and dispose of any assets in the account(s) at FRBNY. When a certification is necessary, Legal will work with the State Department and the country’s Embassy and central bank to obtain a 25(b) certification.

Section 25(b) Certification

Section 25(b) of the Federal Reserve Act allows FRBNY to seek a certification from the State Department. Exemption 7

Exemption 7

Exemption 7

Designations of foreign governments may vary. For example, a foreign government sometimes may wish to designate more than one individual and authorize the designees to act only jointly, and without the right to delegate authority. As this may limit the Bank's ability to conduct business, whenever possible, the Bank may want to seek a less restrictive 25(b) certification. In all cases, FRBNY considerations will include:

Exemption 7

In addition, ARS/AC must consider:

- Whether a new account agreement is advisable. Execution of a new account agreement is advisable to establish and formalize the renewal of the customer relationship. This should include a new tax certification.
- A new telecommunications 'understanding' should be executed. If SWIFT is available in the country, an exchange of Relationship Management Application (RMA) authorizations should occur also.
- A new Automatic Investment program should be established.

Exemption 7

Special Note Concerning OFAC Restrictions:

In addition to obtaining a 25B certification in cases of uncertain ownership and/or management of the account, in cases where assets in the account are blocked pursuant to OFAC regulations, FRBNY will need a license to unblock the funds and resume services. Essentially, the FRBNY may receive one of three different types of licenses:

Internal FR

- A directive license instructing FRBNY to transfer the assets in the account to a certain beneficiary⁸;
- A general license which unblocks the funds, but does not allow FRBNY to resume providing services to the account holder except for a one-time transfer of funds out of the account at the customer's instructions; or
- A general license which unblocks the funds and allows a complete resumption of services.⁹

The main point with respect to the OFAC license is that CBIAS must understand what activity is and is not permitted by the license.

⁸ Additional scenarios regarding OFAC blocking not specific to the account holder relationship are provided in the MOP Section 4 on OFAC and Exemption 7.

⁹ Please also see discussion of Review of Blocked Property Held at FRBNY in the MOP Section 4 on OFAC and Exemption 7.

Section 4: OFAC and Exemption 7

Introduction to OFAC and Exemption 7

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers and authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction.

OFAC Sanction Programs

The basic goal of OFAC sanctions is to prevent sanctioned entities from access to U.S. financial markets. The sanction programs can target a particular country or regime, organization, individual or practice (dealings with conflict diamonds, proliferation of weapons of mass destruction). These programs frequently change and many exemptions exist for each program. At the time of writing, the current OFAC programs were explained as follows:

“Comprehensive sanctions programs include Burma (Myanmar), Cuba, Iran, Sudan and Syria. Other non-comprehensive programs include the Western Balkans, Belarus, Cote d'Ivoire, Democratic Republic of the Congo, Iraq, Liberia (Former Regime of Charles Taylor), Persons Undermining the Sovereignty of Lebanon or Its Democratic Processes and Institutions, North Korea, Sierra Leone, and Zimbabwe as well as other programs targeting individuals or entities that could be anywhere. Those programs currently relate to foreign narcotics traffickers, foreign terrorists, WMD proliferators. In addition to targeted countries, it is very important to note that OFAC publishes a list of Specially Designated Nationals and Blocked Persons ("SDN list") which includes over 6,000 names of companies and individuals who are connected with the sanctions targets and are located throughout the world. A number of the named individuals and entities are known to move from country to country and may end up in locations where they would be least expected. U.S. persons are prohibited from dealing with SDNs wherever they are located and all SDN assets are blocked¹⁰.”

The type of sanctions applied to a particular country, organization, group or individual may vary across sanction programs. Each sanction program is unique and has individual requirements designed to achieve specific goals in foreign policy. For example, a sanction program may:

- Ban all transactions within a given country;
- Restrict only certain activities;
- Require pre-approved licenses;

¹⁰ <http://www.treas.gov/offices/enforcement/ofac/faq/answer.shtml#9>

- Only restrict transactions with specific individuals; or
- Involve blocking, rejecting, or both.

Exemption 7

More detailed information on OFAC history, in-depth descriptions of the individual sanctions program, and the full updated SDN list are available on the OFAC website (<http://www.treas.gov/offices/enforcement/ofac>). Additional OFAC training material is also available Exemption 7

Blocked Transactions

U.S. law requires that certain assets and accounts be blocked when such property is located in the United States, is held by U.S. individuals or entities (wherever located), or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC designated party on the transaction, it must be blocked. It is possible that a FIMA customer may order a payment to, or receive funds into its account that are in some way connected to an OFAC-designated entity. FRBNY must block transactions that are:

- by or on behalf of a blocked individual or entity;
- to or through a blocked entity; or,
- in connection with a transaction in which a blocked individual or entity has an interest.

When the instructions of a funds transfer payment fall into one of these categories, FRBNY must not execute the payment order and place the funds into an interest-bearing blocked account.

Prohibited or Rejected Transactions

Prohibited transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute¹¹. They are distinct from blocked transactions in that it is possible that there is no blockable interest involved (i.e. no SDN involved). In such a scenario, a transaction would be rejected and sent back to the remitter in the case of a receipt and not processed. Exemption 7

Exceptions to the Prohibitions: OFAC Licenses

OFAC regulations often provide general licenses authorizing certain categories of transactions (i.e. payments for humanitarian assistance for a sanctioned country). OFAC also issues specific

¹¹ <http://www.treas.gov/offices/enforcement/ofac/faq/answer.shtml#3>

licenses on a case-by-case basis under certain limited situations and conditions. Please see a list of licenses relevant to CBIAS account activity at [Exemption 7](#).

OFAC Reports and Record Retention

When a transaction is blocked or rejected, FRBNY is required to file a report with OFAC. OFAC requires that all blocking and reject reports be submitted in writing and be accompanied by a copy of the original transfer instructions. OFAC regulations require the retention of all reports and blocked or rejected transaction records for five years. An audit trail for each customer should be created and retained that includes names checked, decisions and reasons behind decisions, and the status of the customer.

Reporting of Transactions that Violate OFAC Regulations

Any transaction that has been blocked or rejected must be reported to OFAC within ten business days from the date the action was taken. The standardized forms required to report these actions are:

- Voluntary Form for Reporting Blocked Transactions
- Voluntary Form for Reporting Rejected Transactions

The reports are completed and sent to OFAC by the Legal Department. Examples of these forms are made available on the OFAC web site.

Annual Report

Blocked property must also be reported to OFAC annually. The Annual Report of Blocked Property is due by September 30 of each year. The report details all of the blocked property as of June 30 of the same year. An archive of past reports can be found at [Exemption 7](#) and Guarded Account – Annual holdings Report OFAC. The information for this report is provided by AC staff and submitted by Legal. OFAC uses this information for planning purposes and to verify compliance. There is no annual reporting of rejected transactions.

Review of Blocked Property Held at FRBNY

As stated above, FRBNY is required to report any blocking of assets to OFAC within ten business days of its occurrence. At the end of the second quarter, FRBNY is also obligated to provide an annual report of blocked property in CBIAS accounts. In addition, FRBNY may be required to submit information, if any, relevant to the U.S. Treasury's Annual Terrorist Assets Report to Congress ("TAR").

As part of the preparation of the Annual Blocked Property Report and/or information relevant to TAR, AC will review the details and supporting documentation for each blocked property item and will contact Legal, and notify Compliance, for review of the item's latest status under the relevant law. This review will allow for a determination whether any of the blocked property could be released for one of the following reasons:

- There is a change in the legal regime governing the blocked property item (such as a revision or amendment of the Executive Order lifting the blocking or change to the OFAC regulation upon which the blocking was based, including OFAC's granting a general license for the release of the funds); or
- A specific license is granted by OFAC to the interested party/owner of property to apply for a license with OFAC for the release of the funds; or
- Any other authorization issued by OFAC that permits release of blocked property.

Importantly, receipt of an OFAC license may not be sufficient for release of the property item by FRBNY. In cases of disputed ownership, FRBNY may consider bringing a legal action to ascertain the ownership of the property.

It also should be noted that AC, Legal and Compliance monitor changes to OFAC regulations throughout the year, and if changes are noted that affect the status of blocked property entries, action will be taken at the time and does not need to wait until the annual review.

If an unblocking opportunity exists through an OFAC license request, AC will forward the necessary information about how to contact OFAC onto interested parties. Where permissible, and on a case-by-case basis, the FRBNY will communicate with the customer or, at customer's request, with another involved party of a transaction for which blocked property exists on FRBNY books if there is a need for the customer and/or the party to follow-up with OFAC on authorizing release of blocked property. AC will log any related communication and follow-up as needed.

Transaction Filtering

The FRBNY is required by law to comply with OFAC regulations and OFAC compliance is a principal objective of AC's compliance efforts. AC monitors FIMA account transaction activity on a real-time basis in effort to comply with OFAC regulations. The goal is to ensure that no OFAC-sanctioned entities are party to transactions in FIMA accounts.

To assist CBIAS in complying with OFAC regulations, AC employs interdiction software called Exemption 7



Exemption 7



Exemption 7



Exemption 7



List Updates and List Management

Exemption 7



Internal FR

Exemption 7



User-added entries

Exemption 7



AC Management will on occasion have a need to add a name to the list as an exception or “good guy.” An exception addition is intended to eliminate excessive false hits that the proposed “good guy” name is generating and eliminate unnecessary volume of manual reviews for analyst if the name is known not to present concerns. This addition to the list tells Exemption 7 that the particular match can be passed. Additions to the “good guy” list are made the same way other user-added entries are made. Exemption 7



Overall Maintenance:

AC will periodically review the need to add rules and exceptions if excessive false hits are being produced.

Transaction Monitoring in Exemption 7

In reviewing a particular transaction, the analyst needs to determine whether it may violate any OFAC regulations, as this may require the funds to be blocked or rejected. Because OFAC sanction programs generally are either country-based or SDN list-based programs, the review should focus on two issues:

- a) Whether the transaction involves a country that is sanctioned by OFAC; and/or
- b) Whether any party in the transaction appears on the OFAC SDN list.

How monitoring is conducted and what we look for

Exemption 7



Exemption 7



Exemption 7



Escalation Procedures:

In accordance with the Bank's OFAC policy, the following escalation procedures should be followed: if there is a potential violation of an OFAC sanctions program, the matter must be immediately escalated to AC management (approver) for review prior to taking any further action. If AC management (approver) determines that a potential OFAC violation exists, such management is responsible for escalating the matter to the OFAC Team. The OFAC Team will conduct an investigation in order to determine whether there is an actual OFAC violation. Once the investigation is complete, the OFAC Team will notify area management of its findings, and will recommend a course of action. In case of a confirmed OFAC violation, the Legal Function will advise whether any filings or reports must be filed with OFAC, and whether other measures (e.g., blocking of assets or rejection of transactions) are necessary.

Note: Incoming items that are flagged for review by Exemption 7 have already been received by the FRBNY under the customer's account. In the event that incoming funds would need to be blocked, the funds in question would need to be manually debited from the account by FSS and credited to a segregated "blocked" account set up by AC. Debit instructions from the customer are not required in the case of an OFAC violation. For more information on blocked accounts, see MOP Section 2. For a comparison of payment and receipt attributes, see Appendix B.

As set forth in the Bank's Anti-Money Laundering Policy (the "AML Policy"), consistent with the business areas responsibilities to manage various operational, legal and compliance risks, business areas also must take measures to reduce money laundering risks, including, but not limited to conducting an appropriate level of transaction monitoring, and escalating unusual or atypical activity.

Exemption 7

Please see Appendix D for additional guidance for identifying these high risk typologies. In addition, as the CBIAS compliance program continues to develop, additional typologies may be identified that cause concern and will be included accordingly.

In addition to post review escalations, the following transactions are escalated to Compliance for real time review: transactions involving possible OFAC related concerns (these are escalated to the Exemption 7), Exemption 7

Exemption 7 and any other transactions that the CBIAS Analyst deems potentially suspicious and would benefit from additional review by Compliance. Compliance will review any escalated transactions, including conducting any additional due diligence required to make a determination regarding the risk posed to the Bank in facilitating such transactions.

Self Testing:

CBIAS conducts its quality control operations on real-time transaction scanning in Exemption 7 by randomly sampling transactions directly passed by analysts and transactions escalated for second-level approval. Exemption 7

The manager responsible for quality control for that period will open the report and verify that each transaction was appropriately processed according to normal Account Control procedures. Deviations from procedures which occurred during the processing of the transaction should be noted by the manager in a separate document. These deviations should be resolved through discussions with the individuals responsible and, if necessary, changes to procedures. If the deviations were required for extenuating circumstances (such as a system failure) this should be noted in the report.

Reference documents:

Internal FR

Exemption 7



Section 5: Compliance Hold

Section 3 of the MOP describes how account/customers are classified as Restricted or Monitored and consequently reviewed under the Compliance Hold status. This section describes how the Compliance Hold review works

Exemption 7

Compliance Hold allows AC analysts to check if transactions present a compliance concern in real time; that payments from Restricted accounts conform to previously-approved account activity in those accounts. Compliance Hold also allows AC staff and management to review and evaluate new activity as it occurs.

How the Compliance Hold queue works: Passing, correcting, and cancelling transactions

Exemption 7

For outgoing payments, if additional information is requested by AC or the Compliance Function in order to better understand the payment, the payment could be revalued on a case by case basis and its processing would be pending the receipt of requested customer information.

To request the correction or cancellation of an item in Compliance Hold:

Exemption 7

Exemption 7



Analyzing Payments in the Compliance Hold Queue

Exemption 7





Section 6: High Scrutiny Monitor

AC anticipates this section will change as AC plans to utilize reporting features of to assist in the preparation of the High Scrutiny Report.

Exemption 7

Introduction

AC circulates the High Scrutiny Monitor (HSM) each day to a diverse audience within the FRBNY, including CBIAS CM, BD, FSS, ARS and AC staffs, the Compliance Function, and members of the Legal Group who work on CBIAS issues. The HSM is an ex-post review (prior business day) of the funds activity for all Restricted and Monitored accounts. A description of the Restricted and Monitored risk categorization is explained in MOP Section 3. As an important component in CBIAS' compliance program, the HSM serves the following purposes:

- Highlight transactions of concern that were not flagged for review on an ex-ante basis;
- Keep informed of interesting and important compliance-related developments;
- Enhance understanding of how Restricted and Monitored customers utilize their accounts with the FRBNY; and,
- Protect the interest of FIMA customers by monitoring for improper account usage and improper transfer of assets in to or out of the accounts.

The HSM involves a review element and a reporting element. While analysts will not report on every transaction they review, the analyst's review of all Restricted and Monitored accounts' activity develops over time into in-depth familiarity with the accounts and their "baseline" activity.

Exemption 7

Preparing the HSM – Automated Tools

AC analysts use three automated tools to prepare High Scrutiny Monitor:

Exemption 7

Exemption 7

Reviewing Transactions

The ex-post review of funds activity in Restricted and Monitored accounts is a critical element of preparing the HSM. Once the analyst has downloaded the Exemption 7 file, they will review the contents with particular focus on compliance risk and whether the activity falls within the bounds of generally-accepted central bank activity.

Reviewing the Transaction Details File to Account for Quantitative Changes in Holdings

Exemption 7

Selecting Items for the Written Highlights

Task: identify items that deserve additional scrutiny and/or provide unique insight into customer account usage.

Analysts select items of interest for a written review that is more detailed than the information provided in the HSM table. General guidelines for selecting items for written review are:

Exemption 7

This list above is not exhaustive above and other transactions of interest could also be noted. For further details on due diligence, please refer to MOP Section 7. In all cases, the details (or lack of details) included in a transaction should also guide an analyst's decision to highlight a transaction in the HSM.

Finally, items that are not of concern, but of note for the reasons outlined above, may be highlighted in the HSM in order to enhance staff knowledge of account activity in general. Some items may require review by AC management prior to inclusion in the HSM, in order to ensure that the information does not violate CBIAS' obligation to maintain the confidentiality of its customers' information.

Creating the Written Highlights

Task: Present highlighted items in a manner that clearly explains relevant details and the reason for its highlighting.

The purpose of highlighting specific transactions for written analysis is to note activity that departs from an account's normal activity, that is of specific compliance concern, or that has received attention from management (and possibly from other areas within the FRBNY) due to considerable concern or uniqueness. This section details how highlighted items should be presented to the HSM audience.

In order to make each highlighted item meaningful to the audience and to develop the collective understanding of how restricted and monitored accounts are utilized, analysts should concentrate on addressing the following points:

- 1.) Explain why the item is being highlighted, particularly by noting what constitutes “normal” activity for the account. If an item strongly resembles typical activity for an account that has been described in a prior HSM, presenting it may not serve to deepen understanding or provide unique insight.
- 2.) Explain whether the item seems to present compliance risk, is of general interest, is inconsistent with official activity, or any combination thereof.

Exemption 7

- 4.) Explain any actions that have been or will be taken by AC, especially planned correspondence or decisions to change the status of the account (i.e. from monitored to restricted). When highlighting an item of continued interest (for example, a payment held in Exemption
7 until sufficient information is received from the customer), be sure to explain the disposition of the item in question.

Exemption 7

Section 7: Due Diligence

Due Diligence for CBIAS Transactions

Conducting due diligence and researching transaction details of CBIAS account activity are critical components of AC's compliance efforts. The purpose of due diligence is to ascertain the compliance and reputational risk that a transaction presents to the Bank to assist in determining a transaction's disposition. Obtaining information about a transaction helps an analyst determine whether the transaction appears to be of an official nature and assists in resolving any specific concerns about the entities and individuals involved or the nature of the payment. This transaction-level due diligence is the foundation for understanding the customer's use of the account¹⁶.

AC's compliance work depends heavily on the analyst's judgment, resourcefulness and analytical skills to locate and integrate diverse sources of information, to determine whether escalating a transaction is necessary, and to make a recommendation to AC management on how to proceed with processing of an escalated payment.

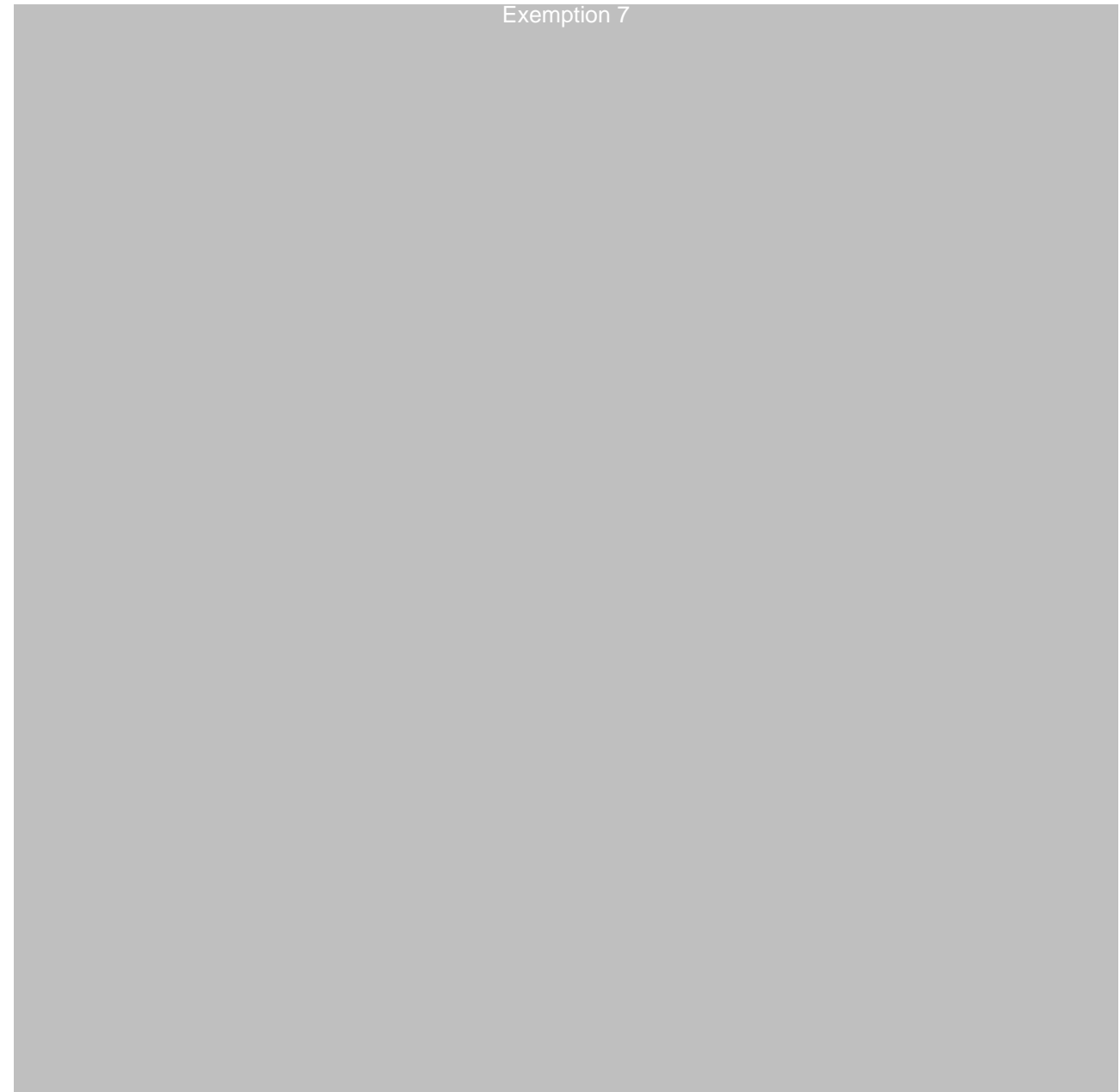
Analysts have many resources available to them for researching transactions and their underlying details, in order to try to resolve suspicions that have emerged in the course of a manual review or Compliance Hold in Exemption 7 or High Scrutiny context. Some of these resources and reference include, but are not limited to the following:

Exemption 7



¹⁶ Further detail on customer-specific (KYC) due diligence is elaborated in MOP Section 02.

Exemption 7



Analysts should ascertain the information source's reliability and credibility before incorporating it into the analysis. Analysts should also use caution when using information from blogs and unknown sites for the danger of malicious code. The analyst should exhaust all reference resources available to them, while considering time constraints and the importance of managing the overall volume of transactions in Exemption 7 and Compliance Hold. If the due diligence burden at hand requires more time than is available, another compliance analyst should be recruited to assist until the transaction volume returns to a manageable level.

The Compliance Function has additional research resources available to them, including Exemption 7, among others.

Overview of [REDACTED] Flow and Inputs
Dated 2012-05-30

Exemption 7

Message Types and

Exemption 7

Dated 2012-03-29

Exemption 7

Compliance : Monitoring Payments vs. Receipts

Exemption 7

Exemption 7

APPENDIX D: ADDITIONAL GUIDANCE FOR IDENTIFYING HIGH RISK TYPOLOGIES

Exemption 7



Exemption 7

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



APPENDIX E- AML RED FLAGS

Exemption 7



Account Management Guidelines

Exemption 7

Account Management Guidelines

Exemption 7

SITUATION A

Exemption 7

Account Management Guidelines

Exemption 7

SITUATION B

Exemption 7

Account Management Guidelines

Exemption 7

SITUATION C

Exemption 7

Compliance's List of AML/CFT Due Diligence Resources

Exemption 7



Exemption 7



Compliance Function

AML MANUAL OF PROCEDURES



Internal F.R.

Compliance Function

Table of Contents

| | | |
|------|---|----|
| I. | Introduction | 3 |
| II. | AML Requirements Applicable to the FRBNY | 3 |
| III. | Applicability & Scope | 4 |
| IV. | Key Terms & Resources | 6 |
| V. | Procedures | 6 |
| A. | AML Monitoring | 6 |
| 1. | Daily Transaction Review | 6 |
| a. | Central Bank and International Account Services (“CBIAS”) | 6 |
| 2. | Lookback Reviews | 7 |
| a. | CBIAS | 7 |
| | Non-Responsive | 10 |
| | | 11 |
| | | 11 |
| 4. | Review of AML Internal Lists | 14 |
| 5. | KYC Profiles | 16 |
| a. | CBIAS | 16 |
| | Non-Responsive | 18 |
| B. | AML Due Diligence..... | 29 |
| C. | Escalation Procedures..... | 44 |
| VI. | Training | 48 |
| VII. | Recordkeeping..... | 48 |

I. Introduction

As scrutiny of anti-money laundering practices in the financial services industry continues to intensify globally, banks and other financial institutions are taking a more active role in combating money laundering and terrorist financing. In response to these risks and the increased focus on internal corporate controls, the FRBNY has implemented an [AML Policy](#)¹ in order to standardize practices and define the roles and responsibilities of its management and staff in upholding the institution's commitment to implement effective money-laundering controls to protect the Bank's reputation and the integrity of the financial system.

All Compliance AML Analysts ("Compliance analysts") are required to be familiar with these procedures and the [Bank's AML Policy](#).

II. AML Requirements Applicable to the FRBNY

The Bank is not subject to the AML requirements applicable to financial institutions under the Bank Secrecy Act and its progeny (collectively, the "BSA"),² and does not offer the full range of services offered by other financial institutions; nevertheless, the services that the FRBNY does offer,³ as well as its unique responsibilities, expose the Bank to similar risks and impels its adherence to the very standard it imposes as part of the Bank's regular safety-and-soundness examination program.⁴

Congress enacted the BSA to protect the U.S. financial system from the abuses of financial crime. Revised and strengthened over the years, criminal money laundering statutes generally make it a crime for any person to conduct a financial transaction or international transportation of funds with the proceeds of specified criminal activities with knowledge (including "willful blindness") that the funds were derived from some form of criminal activity.

¹ Federal Reserve Bank of New York, "Federal Reserve Bank of New York Anti-Money Laundering Policy", Federal Reserve Bank of New York internal website Exemption 7 accessed January 2016. Also, *see, Infra*, Appendix A.

² See Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §§5311-5314, 5316-5324 (Bank Secrecy Act and regulations at 31 C.F.R. Part 103); Money Laundering Control Act (1986), 18 U.S.C. §§1956 and 1957; Anti-Drug Abuse Act of 1988, 31 U.S.C. §5311; Annunzio-Wylie Anti-Money Laundering Act, 31 U.S.C. §5314 (1992); Money Laundering Suppression Act, 31 U.S.C. §5318 (1994); Money Laundering and Financial Crimes Strategy Act, 31 USC §5301 (1998); International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 (USA PATRIOT Act Title III), 31 U.S.C. §5311; Intelligence Reform & Terrorism Prevention Act of 2004, 50 U.S.C. §401.

³ Many of the financial and market services that FRBNY provides to its customers are comparable to the services of commercial banks and broker-dealers. Some of these services, particularly those services that are provided to higher risk customers and involve higher risk jurisdictions, may pose significant money laundering and terrorist financing risks.

⁴ See "Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements," Board of Governors, Federal Reserve System (July 19, 2007).

In order to protect the Bank's reputation, to mitigate and control legal and reputational risks, and to help ensure that the FRBNY abides by sound practices for AML risk management to the extent expected from the banking institutions that it supervises, the Bank has voluntarily elected to adopt and enforce the AML Policy.

III. Applicability & Scope

The Compliance Function (“Compliance”) is an independent function within the Legal Group responsible for identifying the legal and reputational risks associated with the Bank’s activities and for developing and coordinating the implementation of policies and procedures designed to address these risks. In discharging its duties, Compliance regularly reports to senior management and periodically to the Audit Committee of the Board.

By documenting its processes in this manual, Compliance aims to ensure the following:

- **Accountability**: A memorialized set of processes agreed upon by Compliance management will add greater credence to recommendations/observations derived from these processes as well as to future endeavors undertaken by Compliance;
- **Ease of Access**: With clear documentation, a process can continue as designed, and changes can be made in a timely manner that allows Compliance to run effectively in the event of staff turnover;
- **Responsiveness**: The ability to quickly update and disseminate procedures enables Compliance to meet changing Bank needs and to adapt to new environments; and
- **Guidance**: To ensure ongoing commitment and understanding of the AML Policy, Compliance analysts will be able to consult this manual as a source of reference in performing their duties.

Per the Bank’s AML Policy, the Chief Compliance Officer (“CCO”) serves as the Bank’s AML Officer. The CCO and Compliance have responsibility for overseeing and monitoring the development, implementation, and maintenance of the AML program, including review of business area policies. Under the direction of the CCO, Compliance guides and supports each affected business area by:

- Identifying and assessing AML risks specific to the business area;
- Working with the business areas to develop and implement a risk-based AML program, Know Your Customer (“KYC”) profiles, and control activities, such as appropriately tailored AML procedures, including customer due diligence policies and procedures, and parameters for identifying, investigating and referring to Compliance suspicious activity;

- Assessing the AML risk of new Bank products and services and advising business areas on how to best manage and mitigate AML risks;
- Developing and conducting periodic AML training programs;
- Periodically testing the sufficiency of business areas' AML controls;
- Keeping management and the Board apprised periodically of the content and operation of the Bank's AML compliance program and the enforcement of the AML Policy;
- Drafting and maintaining the Bank's enterprise-wide Anti-Money Laundering Manual ("AML Manual"), and
- Reviewing and approving business areas' relevant AML procedures.

Moreover, Compliance is responsible for:

- In consultation with the Legal Function, presenting a mandate to business areas to adopt a comprehensive AML program and develop appropriate AML controls;
- Making recommendations to business areas regarding specific transactions, proposals, or issues, and presenting significant policy questions to the Management Committee or to the Risk Committee;
- Determining what constitutes suspicious activity, including reviewing specific instances of potentially suspicious activity and, with the advice of counsel, reporting it to the relevant government authorities;
- Where appropriate, conducting *post hoc* or ongoing monitoring of potentially suspicious activity;
- Making final determinations regarding policy breaches, including breaches reported from business areas;
- Administrating the annual Compliance Risk Assessment, which includes an evaluation of AML risk;
- Maintaining the Exemption 7 Country Risk Matrix; and
- Managing the Suspicious Activity Monitoring ("SAM") system, including but not limited to, creating monitoring scenarios and rules and reviewing alerts generated by the system.⁵

⁵ Id. at 5.

IV. Key Terms & Resources

1. The [AML Policy](#) was adopted in order to standardize practices and define the roles and responsibilities of the Bank's management and staff in upholding the institution's commitment to implement effective money-laundering controls to protect the Bank's reputation and the integrity of the financial system.
2. The Compliance [website](#) provides information related to the role and responsibilities of the Compliance Function, including Compliance programs aimed at AML, Counterterrorism Financing, and OFAC. In addition, there is information available about Targeted Transactional Reviews. Non-Responsive

V. Procedures

A. AML Monitoring

1. Daily Transaction Review

a. Central Bank and International Account Services ("CBIAS")

The Bank offers accounts and provides financial services to foreign and international monetary authorities (FIMAs), some foreign governments, and other international organizations. The provision of accounts and services serves important System and U.S. Government objectives, but the accounts and activities entail financial, compliance, and reputational risk to the Bank. To address these risks, the operating area of the Bank responsible for managing these accounts – CBIAS – has developed a compliance program to identify, assess, monitor, and report legal, regulatory, and reputational risk with the goal of meeting the following objectives:

- Comply with U.S. laws and regulations relating to OFAC;
- Apply principles of U.S. AML regulations (principally the Bank Secrecy Act);
- Protect the Bank's reputation and avoidance of financial risks associated with the provision of financial services to FIMAs;
- Ensure compliance with court orders and other legal process;
- Ensure compliance with Bank and System regulations and policies;
- Protect the interests of the Bank, including avoiding potential embarrassment, by proactively identifying and responding to potentially sensitive circumstances that could result in a legal claim and/or reputational risk;
- Protect the interests of the Bank's customers by guarding against improper use of a customer's account, and improper transfer of assets out of such accounts; and

- Protect the interests of the Bank, the System and the U.S. Government in their bilateral relations with other nations.

The Compliance Function's role in CBIAS' day-to-day transaction monitoring consists of (1) Review of Real Time Escalated Transactions and (2) Review of Daily Escalation Reports.

1. Review of Real Time Escalated Transactions

User-Added List Based Monitoring: The Exemption 7 application used by CBIAS allows for the inclusion of user-added lists. As such, Compliance has developed, and CBIAS has agreed to include a list of agreed upon terms that, if found within a particular transaction, could potentially result in increased legal and/or reputational risk to the Bank. When Exemption 7 identifies one of these terms within the body of a transaction, CBIAS analysts will escalate the transaction to the Exemption 7 for further review. The Compliance analyst will then review the transaction, conduct additional research as necessary, and advise CBIAS of final disposition of the transaction, which may include the processing of the transaction without incident, or the request for customer outreach for more information.

Intraday Escalation Monitoring: CBIAS will occasionally refer a transaction to Compliance for the purpose of conducting additional due diligence, or requesting Compliance's opinion prior to the processing of the transaction. In these time-sensitive situations, Compliance will do its best to provide CBIAS with the requested assistance in a timely fashion. However, Compliance may ultimately recommend that the transaction be re-valued so that further research can be completed prior to the ultimate disposition of the transaction.

2. Review of Daily Escalation Reports

Ex-Post Monitoring: Compliance receives a list of transactions escalated by CBIAS analysts to CBIAS management for disposition on a T + 1 basis (one day after the transactions take place). Included within this list of transactions are the first level analysts' comments and any research performed, as well as CBIAS management's comments and final disposition. Compliance analysts review both sets of comments and, where necessary, perform additional due diligence in order to ensure that there are no additional compliance concerns associated with those transactions.

In the event that Compliance either disagrees with the disposition, and/or would like to obtain further information surrounding the transaction, it will communicate its concerns with CBIAS in a timely manner.

2. Lookback Reviews

a. CBIAS

Exemption 7

The purpose of the lookback reviews is to ensure that Bank management has knowledge of the nature and purpose of the transactional activity being conducted through FRBNY accounts in order to help guard against possible legal and reputational risks associated with money laundering, terrorist financing, fraud, and unusual or suspicious activity.

While conducting lookback reviews, Compliance typically reviews

Exemption 7

The noteworthy activity that Compliance typically escalates to senior management usually falls under one of the following categories:

Exemption 7

Exemption 7



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive

4. Review of AML Internal Lists

As part of its AML monitoring efforts, Compliance developed internal lists that are used for AML monitoring purposes. Specifically, Compliance currently maintains the following two lists:

- 1) FRBNY Compliance User Added List for Exemption 7 and
- 2) FRBNY Compliance Whitelist

1. **FRBNY Compliance User Added List for Exemption 7** contains names of entities that Compliance identified as concerning. The list contains entity names that are monitored real time or post hoc and are related to the following high-risk activity:

Exemption 7

Exemption 7

2. **FRBNY Compliance Whitelist** contains entity names, associated with high risk activities listed above, that Compliance previously reviewed and determined not to be concerning. Because these entity names tend to appear in transactions repeatedly, this list was created in order to eliminate the need for duplicate research.

Exemption 7

Review of Internal Lists:

Compliance will periodically review the internal lists to determine whether any updates are required. Any updates to the FRBNY Compliance Whitelist should also be reflected on the Exemption 7 site.

SAM System:

With the implementation of the SAM System, which is expected to be completed in 2016, the above lists will be replaced with the following internal lists:

1. **SAM Keywords Lists** which contains Exemption 7 AML related keywords that will generate alerts in the SAM System. The keywords fall into one of the following categories:

Exemption 7

2. **Entity Names List** which will replace the FRBNY Compliance User Added List for Exemption 7. The monitoring of all the terms will be done on post hoc basis; and
3. **FRBNY Compliance Whitelist** which will remain as is.

5. KYC Profiles

a. CBIAS

Background

Exemptions 5 and 7



Template for CBIAS
Customer Profile.pdf

FRBNY Legal Automation Group helped in converting the KYC Profile template from Exemptions 5 and 7 database. The KYC draft template was then moved into production.

The following steps were involved on the part of CBIAS and Compliance analysts to prepare and complete a customer's KYC profile.

CBIAS Responsibilities:

Exemption 7

Exemption 7

16. To print the completed Customer Profile, review all the information and seek clarifications and additional information from Compliance before sign off approval.

Compliance Responsibilities:

Exemption 7

Exemption 7

8. To print the completed Customer Profile, review all the information and seek clarifications and additional information from CBIAS before sign off approval.

Exemption 7

Non-Responsive

Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



Non-Responsive



B. AML Due Diligence

The purpose of due diligence is to determine the compliance and reputational risk that a transaction may present to the Bank and to assist in determining proper disposition. Compliance analysts have many resources available to them for researching transactions and their underlying details, in order to try to resolve concerns. Attached is Compliance's List of AML/CFT Due Diligence Resources.



CF List of AML Due Diligence Resources.c

Compliance analysts should ascertain the information source's reliability and credibility before incorporating it into their analysis. Compliance analysts should also use caution when using information from blogs and unknown sites.

Review of CBIAS Transactions

Conducting due diligence and researching CBIAS transactions are critical components of Compliance's review process. Obtaining information about a transaction helps Compliance analysts determine whether the transaction appears to be of an official nature/in the normal course of the business of the customer and assists in resolving any specific compliance concerns about the entities and individuals involved or the nature of the transaction. In addition, this transaction-level due diligence is the foundation for understanding the customer's use of the account.

Compliance reviews supplement the real time monitoring work performed by CBIAS in their day to day responsibilities and serve as an independent check on the transaction activity. Specifically, Compliance looks to identify transactions related to the following types of high risk activity:

Exemption 7

Red Flags

Attached is a list of red flags that may be suggestive of criminal activity. In addition to the specific red flags outlined in the attached document, Exemption 7



List of AML Red
Flags.docx

For more information on what constitutes suspicious activity, please refer to Section 3.1 of the AML Policy and/or Section C of these Procedures. If a Compliance analyst suspects that a transaction may be suspicious, the analyst should immediately notify his or her manager and provide transaction details along with the summary of due diligence research. Compliance manager(s) will follow the escalation steps set forth in Section C of these Procedures.

Compliance Due Diligence Sources

Exemption 7

Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



Exemption 7



C. Escalation Procedures

The Bank's [AML Policy](#) defines suspicious activity as any transaction, or pattern of transactions that meets any of the following conditions:

- The activity has no business or apparent lawful purpose or is not the type of transaction that the particular customer or third party would normally be expected to engage in, and there is no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction;
- The observed behavior is reasonably indicative of pre-operational planning related to terrorism, money laundering, or other criminal activity; or
- The activity has been previously observed such that an examination of the totality of circumstances reasonably indicates that escalation is warranted.

The [AML Policy](#) requires that if a Bank staff member believes that a particular activity or conduct raises concern, that staff member must immediately escalate the matter to area management for review prior to taking any further action. If area management determines that particular activity is unusual or suspicious, such management is responsible for escalating the matter to the Compliance Function.

Once escalated, the Compliance Function will investigate and determine whether the activity is suspicious.

Escalation of Central Bank and International Account Services (CBIAS) Activity:

1. When Compliance is notified by CBIAS of potentially suspicious activity, the Compliance Function will investigate and determine whether the activity is suspicious.
2. Compliance analyst will conduct due diligence and research on the parties involved in the transaction and present its findings to the Chief Compliance Officer (CCO). For instructions on how to conduct due diligence and research on CBIAS transactions, please see Section B of these procedures.
3. If the CCO determines that the activity is not suspicious, the matter will be closed and the business area will be notified.
4. If the CCO determines the activity to be suspicious, [REDACTED] Exemption 7 [REDACTED], the CCO will consult with Legal regarding possible reporting action as per Section 3.1.4 of the [AML Policy](#).

5. However, if the CCO believes that the activity is suspicious, [Exemption 7], the CCO will consult with Legal prior to making the final determination.”
6. Any activity deemed suspicious will be reported by the CCO after consultation with Legal to the appropriate law enforcement agency.¹⁰

Non-Responsive

Non-Responsive




Non-Responsive



Non-Responsive

VI. Training

Training is an essential part of any AML program, because Bank staff members must adequately understand applicable laws, regulations and internal Bank policies and procedures. The Compliance Function provides periodic AML training to all relevant business areas and staff members. The individual business areas, in consultation with Compliance, may also develop internal training or encourage staff to attend external training programs.

Below are links to two sets of slides Compliance created for internal AML training of CBIAS and  staff members.

Non-Responsive

In addition, all Compliance analysts tasked with AML responsibilities are encouraged to attend internal and external AML training. Internal AML training is often circulated by Compliance managers. For external AML training, Compliance analysts should submit a request to his or her manager with a link to desired training.

VII. Recordkeeping

The [Records Management Policy](#) describes the general standards to be applied with the use and management of records.



Federal Reserve Bank of New York Anti-Money Laundering Policy

Introduction

As scrutiny of anti-money laundering practices in the financial services industry continues to intensify globally, banks and other financial institutions are taking a more active role in combating money laundering and terrorist financing. Contributing to these efforts, the Federal Reserve Bank of New York ("FRBNY" or the "Bank") has adopted this Anti-Money Laundering Policy ("AML Policy" or "Policy") to standardize practices and define the roles and responsibilities of its management and staff in upholding the institution's commitment to implement effective money-laundering controls to protect the Bank's reputation and the integrity of the financial system.

This Policy is generally designed to:

- 1) Educate management and staff periodically with respect to anti-money laundering laws and best practices;
- 2) Institute a system of internal controls to ensure ongoing compliance with this Policy;
- 3) Conduct independent testing and monitoring for compliance; and
- 4) Enable management and staff to identify potentially suspicious activity occurring through the use of Bank services or accounts in order to allow the FRBNY to take appropriate, corrective action.

AML Requirements Applicable to the FRBNY

The Bank is not subject to the AML requirements applicable to financial institutions under the Bank Secrecy Act and its progeny (collectively, the "BSA"),¹ and does not offer the full range of services offered by other financial institutions; nevertheless, the

¹ See Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §§5311-5314, 5316-5324 (Bank Secrecy Act and regulations at 31 C.F.R. Part 103); Money Laundering Control Act (1986), 18 U.S.C. §§1956 and 1957; Anti-Drug Abuse Act of 1988, 31 U.S.C. §5311; Annunzio-Wylie Anti-Money Laundering Act, 31 U.S.C. §5314 (1992); Money Laundering Suppression Act, 31 U.S.C. §5318 (1994); Money Laundering and Financial Crimes Strategy Act, 31 USC §5301 (1998); International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 (USA PATRIOT Act Title III), 31 U.S.C. §5311; Intelligence Reform & Terrorism Prevention Act of 2004, 50 U.S.C. §401.

services that the FRBNY does offer,² as well as its unique responsibilities, expose the Bank to similar risks and impels its adherence to the very standard it imposes as part of the Bank's regular safety-and-soundness examination program.³

Congress enacted the BSA to protect the U.S. financial system from the abuses of financial crime. Revised and strengthened over the years, criminal money laundering statutes generally make it a crime for any person to conduct a financial transaction or international transportation of funds with the proceeds of specified criminal activities with knowledge (including "willful blindness") that the funds were derived from some form of criminal activity.

In order to protect the Bank's reputation, to mitigate and control legal and reputational risks, and to help ensure that the FRBNY abides by sound practices for AML risk management to the extent expected from the banking institutions that it supervises, the Bank has voluntarily elected to adopt and enforce this AML Policy.

Money Laundering and Terrorist Financing

Money laundering and the potential misuse of financial institutions to fund terrorist activity are a major concern to governments and financial institutions around the world.

Money Laundering

Money Laundering is the process of disguising the proceeds of crime to appear legitimate. Money laundering sustains a wide range of criminal activities (e.g., drug trafficking, illegal arms sales, smuggling), but can also involve proceeds of any serious crime including, but not limited to, insider trading, bribery, embezzlement, wire or mail fraud and public corruption.

When a criminal activity generates profit or concerns money, those involved seek ways to control the funds without attracting attention to the underlying activity or individuals involved. They do this by disguising the true source of the proceeds, changing the form of the transaction or moving the funds to a place where they are less likely to attract attention of authorities. Because the objective of money laundering is to return the illegal funds to the individual who generated them, money launderers usually prefer to move funds through stable financial systems.⁴

² Many of the financial and market services that FRBNY provides to its customers are comparable to the services of commercial banks and broker-dealers. Some of these services, particularly those services that are provided to higher risk customers and involve higher risk jurisdictions, may pose significant money laundering and terrorist financing risks.

³ See "[Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements](#)," Board of Governors, Federal Reserve System (July 19, 2007).

⁴ Money Laundering, Frequently Asked Questions," Financial Action Task Force, accessed June 24, 2015, <http://www.fatf-gafi.org/faq/moneylaundering/>

As a result, banks and other financial institutions may be used as unwitting intermediaries by money launderers for the transfer or deposit of funds derived from or directed toward illicit activity.⁵ In attempting to make illicit funds appear legitimate, money launderers may use various bona fide financial services to conceal the true source, destination, or beneficial owner of illegitimate funds. While the money laundering process often entails a series of intertwined payments and fund transfers to and from different accounts, traditional bank services, such as processing wire transfers or accepting or distributing cash, may be used to launder money.

Terrorist Financing

Terrorist financing is the financial support of terrorism or those who support or engage in terrorism in any form. Terrorist financing is commonly defined as the process of raising, storing and moving funds, obtained through illegal and/or legal means, for the purpose of terrorist acts and/or sustaining the logistical structure of a terrorist organization. Like money launderers, those who finance terrorism exploit the financial system to conceal illicit activities. In order to achieve their objectives, money launderers have to obtain and channel funds in an apparently legitimate way. However, while the money involved in the money laundering process originates from a criminal activity and is therefore “dirty,” funds channeled to terrorist groups or individuals may originate from crime and/or legitimate sources. Nevertheless, regardless of the origin of the funds, terrorists use the financial system in a similar way to criminal organizations in order to obscure both the source and the destination of their funds.⁶

Table of Contents

| | |
|--|----|
| 1. Applicability & Scope | 4 |
| 1.1 Roles & Responsibilities | 4 |
| 2. Definitions | 8 |
| 3. Policy Requirements | 9 |
| 3.1 Suspicious Activity Detection and Escalation Obligations | 10 |
| 3.2 Training of Bank Personnel | 12 |
| 4. Exceptions | 12 |
| 5. Consequences for Policy Violation | 12 |
| 6. Record Retention | 13 |
| 7. Related Policies & Resources | 13 |
| 8. Policy Administration Information | 13 |
| 9. Appendices | 14 |
| 9.1 Exemption 7 | 14 |

⁵ Basel Committee on Banking Supervision, Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering, 1 (December 1988).

⁶ Model legislation on money laundering and financing of terrorism (Vienna: United Nations Office on Drugs and Crime (UNODC) and the International Monetary Fund (IMF), 2005).

1. Applicability & Scope

This Policy applies to all business areas that the Compliance Function (“Compliance”) presented with mandates to adopt comprehensive AML programs. As of the date of this Policy, those business areas include:

- **Central Bank and International Account Services (CBIAS)**, which offers correspondent banking and custody services to central banks, monetary authorities and certain international organizations to facilitate their official financial operations. CBIAS, as part of the Markets Group, currently maintains approximately 500 accounts for over 250 foreign and international monetary authorities (“FIMA”);

Non-Responsive

This list is not exhaustive, and each business area within the Bank is responsible for assessing its own AML risk and determining whether it needs to adopt a comprehensive AML compliance program and develop appropriate AML controls, in consultation with the Bank’s Legal and Compliance Functions.

1.1. Roles & Responsibilities

1.1.1. Business Areas

Consistent with their responsibilities to manage various operational, legal and compliance risks, business areas subject to this Policy must take measures to reduce money-laundering risks, where appropriate. Those business areas that have been presented with an AML mandate are responsible for their AML risk and must:

- 1) Identify the AML risks facing their business area and implement control activities designed to address those risks;

Non-Responsive

- 2) Complete the annual Compliance Risk Assessment, which includes an evaluation of AML risk. As part of this process, business areas should have an understanding of their customer base and the type of transactions they process;
- 3) Ensure ongoing compliance with adopted AML policies and procedures, and dedicate appropriate staff and budget resources necessary to maintain and implement those procedures;
- 4) Conduct an appropriate level of transaction monitoring, and escalate potentially suspicious activity identified through monitoring efforts and in the normal course of business. For more information on how to escalate potentially suspicious activity, please refer to Section 3.1.3 Escalating Suspicious Activity of this Policy;
- 5) Provide Compliance with internal audit reports and/or written internal reviews that reference or relate to the business area's AML Program;
- 6) Report to Compliance any AML-related risk events or incidents, including but not limited to operational issues, system related issues or potentially suspicious activity;
- 7) Provide Compliance with copies of business area's AML procedures for review and approval;
- 8) Ensure that local staff receives appropriate AML training on an annual basis; and
- 9) Expediently implement specific recommendations made by Compliance with respect to any transaction, proposal, or issue, or raise the matter with the Group's Executive Vice President for further deliberation.

1.1.2. Compliance Function

The Chief Compliance Officer ("CCO") will serve as the Bank's AML Officer. The CCO and the Compliance Function are responsible for overseeing and monitoring the development, implementation, and maintenance of the Bank's AML program, including the review of business area's AML procedures. Under the direction of the CCO, Compliance will support and advise each affected business area by:

- 1) Identifying and assessing AML risks specific to each business area;
- 2) Working with business areas to develop and implement a risk-based

AML program, Know Your Customer (“KYC”) profiles⁹, and control activities, such as appropriately tailored AML procedures including customer due diligence policies and procedures, and parameters for identifying, investigating and referring to Compliance suspicious activity;

- 3) Assessing the AML risk of new Bank products and services and advising business areas on how to best manage and mitigate AML risks;
- 4) Developing and conducting periodic AML training programs;
- 5) Periodically testing the sufficiency of business areas’ AML controls;
- 6) Keeping management and the Board apprised periodically of the content and operation of the Bank’s AML compliance program and the enforcement of this Policy;
- 7) Drafting and maintaining the Bank’s enterprise-wide Anti-Money Laundering Manual (“AML Manual”); and
- 8) Reviewing and approving business area’s relevant AML procedures.

Moreover, Compliance is responsible for:

- 1) In consultation with the Legal Function, presenting a mandate to business areas to adopt a comprehensive AML program and develop appropriate AML controls;
- 2) Making recommendations to business areas regarding specific transactions, proposals, or issues, and presenting significant policy questions to the Management Committee or the Risk Committee;
- 3) Determining what constitutes suspicious activity, including reviewing specific instances of potentially suspicious activity and, with the advice of counsel, reporting it to the relevant government authorities;
- 4) Where appropriate, conducting *post hoc* or ongoing monitoring of potentially suspicious activity;

9

Non-Responsive

Procedures for establishing new account relationships for accounts maintained by CBIAS (i.e. accounts for central banks, foreign governments and international financial organizations), are set forth in Section 2: CBIAS Account Relationships of CBIAS’ Manual of Compliance Procedures.

- 5) Making final determinations regarding policy breaches, including breaches reported from business areas;
- 6) Administering the annual Compliance Risk Assessment, which includes an evaluation of AML risk;
- 7) Maintaining the Exemption 7 Country Risk Matrix¹⁰; and
- 8) Managing the Suspicious Activity Monitoring (“SAM”) system, including but not limited to, creating monitoring scenarios and rules and reviewing alerts generated by the system.

1.1.3. Legal

The CCO reports directly to the Executive Vice President and General Counsel ("General Counsel") of the Bank. When determining whether activity is suspicious, Compliance will consult with the Legal Function, as set forth in Section 3.1.3 Escalating Suspicious Activity of this Policy, and before filing a suspicious activity report or contacting the appropriate Administrative Reserve Bank (“ARB”)¹¹, the appropriate bank regulatory agency or the appropriate law enforcement agency regarding suspicious activity. Legal counsel will assist the CCO by providing legal advice regarding applicable regulations and advising the local business areas in their responsibilities.

1.1.4. Internal Audit Function

The Internal Audit Function (“Internal Audit”) currently assesses AML risks within the operations of the Bank. Based on Internal Audit’s assessment of the risks, periodic reviews of relevant business areas will be performed to determine compliance with the AML regulatory requirements, as outlined in this Policy. To the extent possible, without compromising the independence of either function, Compliance and Internal Audit¹² will coordinate efforts to share information to ensure the common goal of bank-wide AML compliance.

Exemption 7

¹¹ Administrative Reserve Bank (“ARB”) is the Reserve Bank in the Federal Reserve District in which the Financial Institution is located that oversees the administration of Federal Reserve credit, reserves, and risk management policies for a Financial Institution’s operations nationwide. [Accounting Standard Operating Procedure 10.0](#), “2.0 Reserve Bank Roles and Responsibilities.” accessed August 2015

Non-Responsive

1.1.5. Bank Management

The Management Committee (which consists of the Bank President, First Vice President, and all of the Executive Vice Presidents) is responsible for effective management of the Bank's compliance risk, including:

- Ensuring that compliance with laws, rules and standards are followed;
- Ensuring that Compliance Function policies are observed, which entails responsibility for ensuring that appropriate remedial or disciplinary action is taken if breaches are identified; and
- Informing the Compliance Function if compliance incidents occur.

The Management Committee may delegate certain of its responsibilities to the Risk Committee.¹³

2. Definitions

The following definitions are provided to support a common understanding and standard use of terminology used in this Policy.

Financial Crimes Enforcement Network (“FinCEN”) is a bureau of the U.S. Department of the Treasury whose mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti Money Laundering (BSA/AML) Examination Manual¹⁴ was developed to provide guidance on risk-based policies, procedures, and processes for banking organizations to comply with the BSA and safeguard operations from money laundering and terrorist financing.

Know Your Customer (“KYC”) Profile provides baseline for a particular customer's account activity. It is an important tool in identifying deviations from regular transaction activities, which can indicate potentially suspicious activity and give raise to a duty to undertake further inquiry or escalation obligation pursuant to Section 3.1 of this Policy.

¹³ The Risk Committee supports the Management Committee's principal role in guiding and executing the Bank's strategic priorities by bringing greater integration, alignment, and efficiency to the Bank's consideration of risk management issues and provide leadership in implementation. The Risk Committee provides a forum and is charged by the Management Committee to resolve conflicts in the implementation of the enterprise risk framework and risk appetite statement that cannot be resolved through established processes, such as issues that may arise between Control functions (e.g., Compliance and Risk Functions) and the business areas.

¹⁴ For more information about the FFIEC, please visit FFIEC's website: <https://www.ffiec.gov/about.htm>

Money Laundering is the processing of criminal proceeds to disguise their true origin and ownership in order to legitimize the ill-gotten gains of crime. It occurs in three stages:

1. **Placement** is the initial injection of the illegally derived funds into the financial system or carrying the proceeds of crime across borders;
2. **Layering** involves conducting additional, legitimate transactions with illicit funds to attenuate and further separate the funds from their original, illegal source to make it more difficult to trace these funds to the illegal source; and
3. **Integration** is the injection of the illegal funds into the legitimate economy and financial system. The funds now appear as clean or originating from legitimate sources, which substantially reduces the likelihood of raising suspicion that might trigger investigation and prosecution.

Not all three stages are required to be present for the activity to be considered money laundering.

Suspicious Activity Monitoring (“SAM”) system is an automated AML monitoring system that will significantly expand the Bank’s transaction monitoring capabilities, identify money laundering, terrorist financing, fraud, and potentially suspicious activity.

Suspicious Activity Report (SAR) is a document that financial institutions must file with FinCEN following a suspected incident of money laundering or fraud. These reports are required under the BSA.

3. Policy Requirements

Each business area within the Bank that is presented with a mandate is responsible for adopting a comprehensive AML Program and developing appropriate AML controls, in consultation with the Bank’s Legal and Compliance Functions.

The Bank takes pride in the character and integrity of its staff, and holds each staff member to the highest standard of conduct. Accordingly, no staff member will:

- 1) Knowingly launder money or assist another in laundering money, or engage in, or assist another in, other criminal or suspicious transactions; nor,
- 2) Consciously disregard facts that raise a reasonable suspicion that Bank services or accounts are being used for money laundering, or other criminal or suspicious activity.

Additionally, staff members will abide by bank-wide and business area policies

and procedures to help protect against money laundering and terrorist financing activity in Bank accounts and services.

3.1. Suspicious Activity Detection and Escalation Obligations

3.1.1. What is Suspicious Activity?

Suspicious activity is any transaction, or pattern of transactions that meets any of the following conditions:

- The activity has no business or apparent lawful purpose or is not the type of transaction that the particular customer or third party would normally be expected to engage in, and there is no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction;¹⁵
- The observed behavior is reasonably indicative of pre-operational planning related to terrorism, money laundering, or other criminal activity;¹⁶ or
- The activity has been previously observed such that an examination of the totality of circumstances reasonably indicates that escalation is warranted.

3.1.2. Red Flags

Red flags are transactions or other activities that appear suspicious or are otherwise unusual or extraordinary for a specific account. Banks must apply additional scrutiny when they detect red flags in order to determine whether the activity amounts to suspicious activity under the BSA, which could include a bank investigation into the background or purpose of the activity.

While red flags may trigger Bank staff members to perform heightened scrutiny of certain activity – and could lead to an eventual determination that the activity is suspicious – a determination that an activity is unusual is not a determination that suspicious activity has taken place.

Staff members who detect red flags should follow escalation procedures outlined in Section 3.1.3 Escalating Suspicious Activity of this Policy.

For an illustrative list of red flags, please see Appendix A of the Bank's AML

¹⁵ FFIEC, "Bank Secrecy Act Anti-Money Laundering Examination Manual,"

http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm, accessed February 2012.

¹⁶ Congressional Research Service (CRS) Reports and Issue Briefs, "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative," November 1, 2009, via LexisNexis, accessed January 2012.

Manual.

3.1.3. Escalating Suspicious Activity

If a Bank staff member believes that a particular activity or conduct raises concern under this Policy, that person must immediately escalate the matter to area management for review prior to taking any further action. If area management determines that particular activity is potentially suspicious, such management is responsible for escalating the matter to the Compliance Function (specifically, the ^{Exemption 7} ¹⁷ distribution list or the ^{Exemption 7}) in accordance with this Policy.

Once escalated, the Compliance Function will investigate and determine whether the activity is suspicious. If the CCO determines that the activity is not suspicious, the matter will be closed and the business area will be notified. If the CCO determines the activity to be suspicious, ^{Exemption 7} , the CCO will consult with Legal regarding possible reporting action as per Section 3.1.4 of this Policy. However, if the CCO believes that the activity is suspicious, ^{Exemption 7} the CCO will consult with Legal prior to making the final determination.

3.1.4. Reporting Suspicious Activity

For all activity determined to be suspicious, the CCO will consult with Legal to determine whether a Suspicious Activity Report (“SAR”) should be filed or whether the matter should be reported to the appropriate ARB, the appropriate bank regulatory agency or the appropriate law enforcement agency.

With respect to business areas in scope for this Policy, the following course of action will be taken:

- **CBIAS:** given the sensitivity surrounding CBIAS accounts, any activity deemed to be suspicious will be reported by the CCO to the appropriate law enforcement agency; and

Non-Responsive

¹⁷ ^{Exemption 7} is a distributions list consisting of the members from the Compliance Function. The distribution list may be contacted by typing ^{Exemption 7} into the Bank’s e-mail system.

Non-Responsive

Non-Responsive

3.2. Training of Bank Personnel

Training is an essential part of any AML program, because Bank staff members must adequately understand applicable laws, regulations and internal Bank policies and procedures. The Compliance Function provides periodic AML training to all relevant business areas and staff members. The individual business areas, in consultation with Compliance, may also develop internal training or encourage staff to attend external training programs. In addition, individual business areas are responsible for ensuring that all staff members tasked with AML responsibilities are familiar with the business area's AML procedures.

4. Exceptions

There are no exceptions to this Policy. All business areas in scope for this Policy and presented with a mandate are responsible for developing and adopting comprehensive AML programs and appropriate AML controls.

For any questions regarding the applicability of this Policy, please contact the members of the AML Team.

5. Consequences for Policy Violation

Money laundering is a crime. Because of the reputational and financial risks to the Bank posed by money laundering, FRBNY expects and requires each staff member to comply this Policy. Any staff member who fails to adhere to this Policy may be subject to the full range of disciplinary actions up to and including termination and may be subject to criminal prosecution.¹⁹

If a Bank staff member suspects that another staff member may have breached the AML Policy, he or she should report the incident to a member of management or the AML Team. If uncomfortable reporting the alleged violation to a member of management or the AML Team, he or she should call the FRBNY Integrity Hotline at 1-877-52-FRBNY (1-877-52-37269) and report the matter through that channel.

¹⁹ 18 U.S.C. § 1956 (Violations of Section 1956 are punishable by imprisonment of not more than 20 years).

6. Record Retention

Business areas are required to maintain adequate records and documentation supporting business area's AML processes, including documenting the key controls that mitigate AML risks. In addition, business areas should adhere to the Bank's [Records Management Policy](#) and the Bank's [Functional Retention Schedule](#) ("FRS").

7. Related Policies & Resources

In addition to the Policy, business areas should be familiar with the following Bank Policies:

- 7.1 [Compliance Policy](#) establishes a program for achieving compliance with all legal requirements applicable to the FRBNY as well as the bank's standards, policies and procedures.
- 7.2 [FRBNY OFAC Policy](#) establishes guidelines for compliance with U.S. economic sanctions administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), including regulations issued by OFAC.
- 7.3 [High Risk Accounts Policy](#) provides a risk based approach for identifying and mitigating legal risks and reputational risks posed by providing services to certain financial institutions.
- 7.4 [FRBNY Records Management Policy](#) describes the general standards to be applied with the use and management (i.e., creation, identification, retention, retrieval, and disposition or destruction) of records.
- 7.5 [Required Reporting to the General Auditor](#) describes various types of irregular occurrences and operational developments that should be reported directly to the Bank's General Auditor.

8. Policy Administration Information

| | |
|------------------------|---|
| Effective Date: | October 7, 2015 |
| Last Updated: | September 11, 2015 |
| Policy Owner: | Compliance Function |
| Policy Contact: | Refer to Business Owner Listing |

9. Appendices

Exemption 7



Exemption 7



Exemption 7





Federal Reserve Bank of New York Office of Foreign Assets Control (OFAC) Policy

This Compliance Policy establishes guidelines for compliance with U.S. economic sanctions programs administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), including regulations issued by OFAC.

Policy Owner Chief Compliance Officer
Martin C. Grant

Effective Date July 6, 2012

Related Documents:

| Title | Contact |
|---|--|
| Office of Foreign Assets Control - Sanctions Programs and Information | Please visit: http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx |

Table of Contents

| | |
|--|---|
| Part One: Purpose and Scope | 1 |
| ▪ Introduction and Purpose..... | 1 |
| ▪ Scope..... | 2 |
| Part Two: Roles and Responsibilities | 3 |
| ▪ Business Areas | 3 |
| ▪ Compliance Function..... | 3 |
| ▪ Legal Function..... | 3 |
| Part Three: Escalation and Reporting | 4 |
| ▪ Escalation..... | 4 |
| ▪ Reporting to OFAC | 4 |
| ▪ Annual Reporting to Compliance | 4 |
| Part Four: OFAC Overview | 5 |
| ▪ OFAC Sanctions Programs | 5 |
| ▪ Prohibited Transactions..... | 6 |
| ▪ Exceptions to the Prohibitions | 6 |
| Part Five: OFAC Screening Software and Training of Bank Personnel | 7 |
| ▪ OFAC Screening Software | 7 |
| ▪ Testing of OFAC Screening Software..... | 7 |
| ▪ Personnel Training | 7 |
| Part Six: Information and Guidance | 8 |

Part One: Purpose and Scope

Introduction and Purpose

The purpose of this Policy is to establish guidelines for business areas and employees of the Federal Reserve Bank of New York (the “Bank”) in connection with their compliance with U.S. economic sanctions programs administered by the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC), including regulations issued by OFAC. The primary goal of OFAC sanctions is to isolate certain targeted governments, individuals or entities¹ and prevent their access to the U.S. financial system. OFAC administers a number of economic sanctions programs,² some of which target designated individuals or entities and some of which target entire geographic regions.

All U.S. persons,³ including the Bank, must comply with OFAC regulations. Some OFAC rules restrict or prohibit engaging in transactions or dealings with certain designated individuals and entities (as well as entities owned or controlled by them), including those that appear on certain lists that OFAC issues periodically, and others restrict or prohibit engaging in transactions or dealings involving certain geographic areas or the governments in control of certain geographic areas. In some cases, OFAC regulations require assets associated with a particular transaction or account to be blocked, meaning that assets must be frozen on the Bank’s books until OFAC modifies the relevant sanctions or otherwise authorizes or directs the Bank to move the assets elsewhere. In other cases only rejection of transactions is required (rather than blocking), but in either case the matter must be reported to OFAC. OFAC has the power to impose significant penalties on those who are found to be in violation of the programs it administers.⁴

¹ Examples of targeted individuals and entities include narcotics traffickers, individual terrorists, foreign terrorist organizations and persons associated with them, persons who have engaged in activities related to the proliferation of weapons of mass destruction, and persons that threaten national security, human rights, or other U.S. policy interests.

² A full list of OFAC sanctions programs is published on OFAC’s website at the following address: <http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

³ Although it may vary by program, “U.S. person” is generally defined in OFAC’s regulations as any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person physically located in the United States.

⁴ Failure to comply with OFAC regulations may subject the Bank to fines, criminal penalties, adverse publicity and reputational risk, and may subject the responsible employee to a full range of disciplinary actions up to and including termination of employment. The fines for non-compliance can be substantial. Depending on the sanctions program, criminal penalties can include fines ranging from \$50,000 to \$10,000,000 and imprisonment ranging from 10 to 30 years for willful violations. Civil penalties range from \$250,000 or twice the amount of each underlying transaction to \$1,075,000 for each violation. “OFAC Frequently Asked Questions and Answers,” <http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx#11>, accessed December 2011.

This Policy has six parts. Part One describes the purpose and scope of this Policy. Part Two sets forth the general roles and responsibilities of the Bank's business areas, the Compliance Function, and the Legal Function. Part Three provides guidance to be followed with respect to escalation and reporting requirements. Part Four provides further background information and a high-level description of how OFAC sanctions programs are generally structured. Part Five discusses OFAC screening software and training of bank personnel. Finally, Part Six advises whom to contact, if a business area is confronted with an OFAC-related issue.

Scope

Individual business areas within the Bank which engage in transactions or conduct business with third parties outside the Bank are responsible for adopting and maintaining appropriate OFAC compliance and screening procedures, in consultation with the Bank's Legal and Compliance Functions, as appropriate. OFAC compliance and screening procedures developed by an individual business area may be tailored to address the particular risks and operational structure of that business area, but all procedures should reflect the premise that accurate OFAC risk identification and assessment is essential to an effective OFAC program.

As of the date of this Policy, the following business areas have OFAC compliance and/or screening procedures in place:

- **Central Bank and International Account Services (CBIAS)**, part of the Markets Group, screens all incoming and outgoing funds and securities transactions processed on behalf of accounts held at the Bank by central banks, monetary authorities, foreign governments and certain international organizations;

Non-Responsive

It is important to note that this list is not exhaustive, and each business area within the Bank is responsible for assessing its own OFAC risk and determining whether it needs to develop and maintain OFAC compliance and screening procedures, in consultation with the Bank's Legal and Compliance Functions.

Part Two: Roles and Responsibilities

Business Areas

Individual business areas within the scope of this Policy are responsible for establishing OFAC procedures and controls that are in compliance with OFAC programs, and dedicating appropriate staff and budget resources to maintaining and implementing those procedures, including real-time or periodic screening of transactions, counterparties or account-holders, as applicable. Business areas are responsible for performing an initial investigation of potential OFAC violations in their area, and if necessary, escalating the matter to members of the [redacted] Exemption 7 distribution list⁵ ("OFAC Team") as described in Part Three of this Policy.

Compliance Function

The Compliance Function is responsible for independently assessing compliance risks, developing compliance policies and programs aimed at reducing compliance risks, conducting monitoring and testing of controls, enhancing the compliance activities of business areas within the Bank, and fostering awareness of compliance issues. Part of this responsibility includes helping individual business areas develop procedures and controls to ensure compliance with Bank policies, including this Policy. The Compliance Function is primarily responsible for ensuring that a business area's compliance with this Policy is effective by investigating potential matches to OFAC's Specially Designated Nationals and Blocked Persons ("SDN") list, performing a second level of review of OFAC screening processes, assisting business areas in resolving outstanding investigations, and performing periodic assessments of the business area's screening and escalation procedures.

Legal Function

The Bank's Legal Function is responsible for providing legal interpretations of the various requirements imposed by OFAC sanctions programs, including those requirements imposed by OFAC regulations. This includes investigation and interpretation of potential geography-based OFAC matches and providing general guidance on OFAC-related issues. The Legal Function is also responsible for reporting blocked or rejected transactions or assets to OFAC in accordance with the Bank's legal obligation to do so under OFAC's regulations.

⁵ [redacted] Exemption 7 is a distribution list consisting of members from the Bank's Legal and Compliance Functions. The distribution list may be contacted by typing [redacted] Exemption 7 into Bank's e-mail system, or from outside the Bank by emailing [redacted] Exemption 7

Part Three: Escalation and Reporting

Escalation

If a Bank employee believes that a particular transaction, counterparty or account-holder may present a potential violation of an OFAC sanctions program, the matter must be immediately escalated to area management for review prior to taking any further action. If area management determines that a potential OFAC violation exists, such management is responsible for escalating the matter to the OFAC Team in accordance with this Policy and, if applicable, the business area's own OFAC procedures.⁶ The OFAC Team will conduct an investigation in order to determine whether there is an actual OFAC violation. Once the investigation is complete, the OFAC Team will notify area management of its findings, and will recommend a course of action. In case of a confirmed OFAC violation, the Legal Function will advise whether any filings or reports must be filed with OFAC, and whether other measures (e.g., blocking of assets or rejection of transactions) are necessary.

Reporting to OFAC

In general, any transaction or assets that have been blocked or rejected must be reported to OFAC within ten (10) business days from the date the action was taken. OFAC generally requires the retention of all reports and blocked or rejected transaction records for a period of five (5) years. Institutions that hold any blocked assets also must report such assets to OFAC annually. The Bank's Legal Function will submit all such reports to OFAC and will provide copies to the Compliance Function and the relevant business area(s). In addition, OFAC requires notification if it is discovered that an unreported OFAC violation occurred in the past. If such a violation is discovered by a Bank employee, they must immediately notify the OFAC Team. The OFAC Team will conduct an investigation and, in case of a confirmed OFAC violation, the Legal Function will report the violation to OFAC.

Annual Reporting to Compliance

Not less than annually, relevant business areas will provide to the Compliance Function (i) all internal audit reports and/or written internal reviews that reference or relate to the business area's OFAC compliance program, and (ii) a list of all OFAC-related risk events or incidents tracked in Exemption
7 or a similar risk event tracking program. These periodic reports will provide the Compliance Function with information about any risk events or incidents associated with the business area's OFAC compliance program.

⁶ In the case of a business area whose organizational structure involves operational accountability to other Reserve Banks or third parties (such as a fiscal principal), the OFAC procedures applicable to that business area may provide for a different escalation protocol than that specified in this section. Business areas should consult with both the Legal and Compliance Functions if they believe that a different escalation protocol is appropriate.

Part Four: OFAC Overview

OFAC Sanctions Programs

As noted above, OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction. The sanctions can be either comprehensive or selective, using the blocking of assets and certain restrictions on transactions to accomplish foreign policy and national security goals.

The type of sanctions applied to a particular country, organization, group or individual may differ across sanctions programs. Each sanctions program is unique and has individual requirements designed to achieve specific goals in foreign policy. For example, a sanctions program may:

- ban all transactions within a given country
- restrict only certain activities
- require pre-approved licenses issued by OFAC
- restrict transactions with specific individuals
- involve blocking assets, rejecting transactions or dealings, or both

Overall, OFAC sanctions typically prohibit, or at least restrict, U.S. persons from doing business with designated individuals, groups, companies, or countries. Activities that may be restricted include imports, exports (including exports of financial services), travel and financial transactions, including transfers of funds.

OFAC also maintains a consolidated list of “Specially Designated Nationals and Blocked Persons” or “SDNs.”⁷ U.S. persons are generally prohibited from dealing with SDNs and entities owned or controlled by SDNs, and generally the assets of SDNs and owned or controlled entities that are or come under the control of any U.S. person must be blocked. U.S. persons also must reject transactions with members of the Palestinian Legislative Council (“PLC”)⁸ who were elected to the PLC on the party slate of Hamas, so long as the transaction is

⁷ The SDN list contains information about (i) individuals and entities that are owned or controlled by, or acting for or on behalf of, the governments of target countries, and (ii) individuals, groups, and entities designated under sanctions programs that are not country-specific, such as anti-terrorism, diamond-trading, counter narcotics trafficking, and non-proliferation. The SDN list is periodically updated based on changes in foreign policy. The SDN list is published on OFAC’s website at the following address: <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>.

⁸ The list of targeted PLC members identified by OFAC is published on OFAC’s website at the following address: http://www.treasury.gov/resource-center/sanctions/Terrorism-Proliferation-Narcotics/Documents/plc_list.txt.

not required to be blocked because the individual is also an SDN. In addition, pursuant to its Iranian Financial Sanctions program, OFAC maintains a separate list of foreign financial institutions subject to 31 CFR Part 561 (the "Part 561 List"), which describes certain prohibitions or conditions applicable to certain sanctioned foreign financial institutions.⁹

When there are significant changes in OFAC sanctions programs, the OFAC Team will provide timely written guidance to all relevant business areas.

Prohibited Transactions

Prohibited Transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute, regulation or executive order. Because each program is based on different foreign policy and national security goals, prohibitions may vary between programs.

Blocking a transaction involves accepting or segregating the funds or securities intended for the transaction and then freezing those funds, securities or accounts so that the owner is effectively denied access until appropriate action is taken by OFAC. Blocking can occur when a transaction is initiated at an institution or when funds or securities are moved through an institution during a transfer. OFAC generally stipulates that blocked assets be placed into a segregated account in which a reasonable rate of interest is accrued. Individual business areas should discuss this requirement with their accounting area, in consultation with the Bank's Legal and Compliance Functions.

Rejecting a transaction entails refusing to conduct or participate in the transaction, including the refusal to execute an outgoing payment order or, in some cases, returning funds or securities that have been received. Rejecting can occur when a transaction is initiated at an institution or when funds or securities are moving through an institution in a transfer.

OFAC sanctions programs are constantly subject to change and can vary significantly from one program to another, and each program has unique and often complex restrictions, exceptions, and reporting rules. As a result of this variation and complexity, it is important to consult with the Bank's OFAC Team when addressing particular problems, questions or issues.

Exceptions to the Prohibitions

OFAC regulations often provide general licenses authorizing the performance of certain categories of dealings or transactions, and certain statutes or executive orders related to a particular program may explicitly provide for certain exceptions to the restrictions imposed. For example, a general license issued under a specific sanctions program may authorize transactions related to the conduct of the official business of U.S. Government, or it may authorize certain family remittances under the conditions set forth in the general license.

⁹ As of the date of this Policy, the Part 561 List is not yet available. Once available it will be located on the Iran sanctions page of OFAC's web site.

In addition, OFAC also has the authority to issue specific licenses on a case-by-case basis which authorize certain dealings or transactions under certain specified conditions. OFAC may also issue directive licenses which legally compel an individual or entity to take certain actions, such as the movement of blocked assets or the initiation of a transaction that is otherwise prohibited. Bank employees should contact the OFAC Team with any questions about a general, specific, or directive license.

Part Five: OFAC Screening Software and Training of Bank Personnel

OFAC Screening Software

There are numerous interdiction software packages that are commercially available. They vary considerably in cost and capabilities. As a result, selection of new or replacement of existing interdiction software requires review and approval by the Compliance Function. In addition, business areas should notify the Compliance Function of any custom updates (deletions or additions) to the interdiction software's dictionary, and any changes to the interdiction software's screening parameters (i.e., the sensitivity level of the software's screening algorithm) require review and approval by the Compliance Function.

Testing of OFAC Screening Software

Periodically, but at least once a year, the Compliance Function tests the sufficiency of the interdiction software currently in use by any business area (i.e., the methods and parameters being used to conduct OFAC screening, and the types of information and fields being screened). The goal of this testing is to assess the software controls put in place to ensure that the business area's OFAC procedures are being followed, and to confirm that such controls allow the business area to sufficiently address OFAC requirements. Results of the testing reviews, including any exceptions noted, are reported to senior management and the Bank's Chief Compliance Officer, who may inform the Board's Audit Committee and the Bank's Management Committee if appropriate. In addition, the Compliance Function requires prompt follow-up from a business area to ensure that appropriate corrective action is taken with respect to any weaknesses identified or recommendations made in connection with this periodic testing.

It should be noted that this testing is separate from, and is not a substitute for, any independent review performed by the Bank's Internal Audit Function.

Personnel Training

Training is an essential part of any OFAC compliance program put in place by any business area, because employees must adequately understand applicable laws, regulations, and internal Bank policies and procedures. The Compliance Function provides periodic training to all relevant employees and business areas. The individual business areas, in consultation with the Compliance Function, may also develop internal training or encourage staff to attend external training programs.

Part Six: Information and Guidance

Bank employees should err on the side of caution if confronted with an OFAC-related issue and should consult with the Bank’s Legal and Compliance Functions for further guidance before taking any action. For information and guidance regarding this Policy, please e-mail the [redacted] team [redacted] or contact any of its members listed below:

Compliance Function

[redacted] Exemption 7

Legal Function

Financial Services, Technology and Contracts Division

[redacted] Exemption 7

Exemption 7



Exemption 7

AML Red Flags

1. CBIAS Red Flags

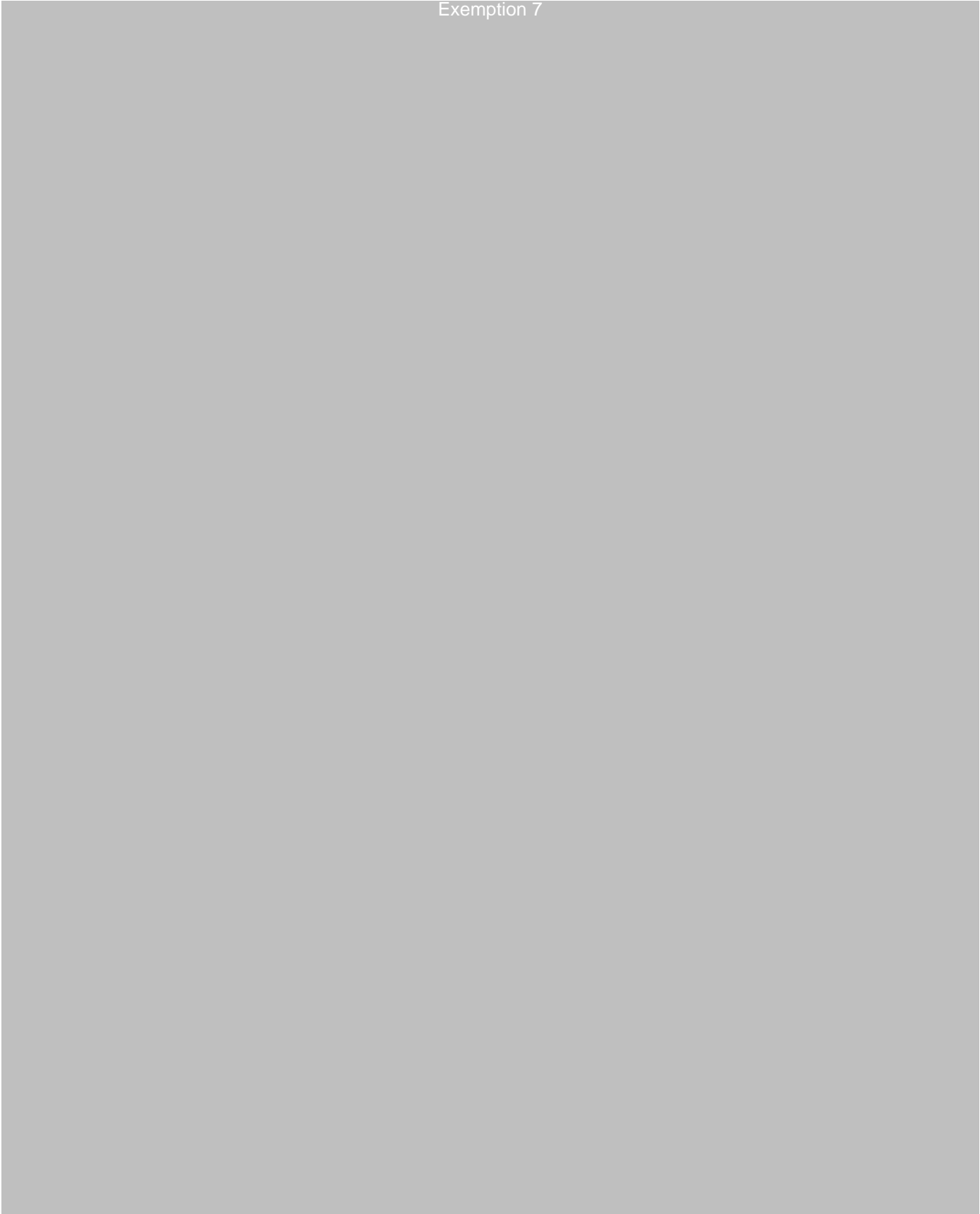
Exemption 7



Exemption 7



Exemption 7



Exemption 7

Exemption 7

Exemption 7

Exemption 7



Exemption 7



Establishing a New Account Relationship

Federal Reserve Policy

The Federal Reserve Bank of New York is the only Reserve Bank in the Federal Reserve System that maintains account relationships with other central banks, foreign governments and international financial organizations, and does so on behalf of the System. In general, account holders at the Bank are limited to:

Board Approved, or "Regulation N" Accounts: Institutions with Central Banking Responsibilities

The authority to establish accounts for 'foreign banks or bankers, or foreign states' is found in the Federal Reserve Act although the criteria used in recommending the opening of accounts for foreign and international institutions is generally more restrictive than this basic provision. The earliest accounts at the Bank were established for its central banking counterparts (such as the Exemptions 4, 7, and 10). The foreign customer base eventually expanded to include those institutions such as currency boards and governmental financial entities, that, while not strictly central banks, exercised central banking functions, particularly in the management of official foreign exchange reserves (such as Exemptions 4, 7, and 10). Accounts have also been opened for international or regional institutions that have characteristics comparable to central banks. Examples of such "central banking institution" accounts are those for the Exemptions 4, 7, and 10.

The approval of the Board of Governors of the Federal Reserve System is required by the Federal Reserve Act, as amended by Regulation N, to establish these accounts. In addition to accounts for those organizations with central banking responsibilities, included in these 'Regulation N' accounts are those Exemptions 4, 7, and 10.

Accounts Established by Statute or Executive Order: International Official Financial Organizations

Accounts are established for certain international or regional financial institutions which are not similar to central banks but of which the United States is a member. These accounts, Exemptions 4, 7, and 10, are generally established pursuant to a request authorized by statute, which, in establishing U.S. membership, also specifies that any Federal Reserve Bank shall act as its depository or fiscal agent.

Other accounts for international and regional organizations have been opened in cases where these organizations (1) had multinational official sponsorship, (2) were designed to contribute to financial order, and (3) contemplated operations consistent with public policy in the U.S. and the purposes of the Federal Reserve, and would have transactions of such a size or nature to make handling by the Federal Reserve essential, or importantly convenient, to both the institution and the Federal Reserve.

Accounts Established at the Request of the Treasury Department: Fiscal Agency Accounts

Certain accounts, such as those for official international or regional institutions whose responsibilities are not mainly financial, such as Exemptions 4, 7, and 10 have been opened only at the specific request of the U.S. Treasury.

Account Request Process Flow Chart

Exemptions 4, 7, and 10



Procedures for Establishing 'Regulation N' Account Relationships

On receipt of a request from an institution to establish an account at the Federal Reserve Bank of New York:

1. With CBIAS management and in consultation with the Compliance Function (in regard to country risk ratings) review the Exemption 7

2. Based on this research, determine if the organization is eligible to establish an account at the Bank, *in terms of its legal status (insofar as no concerns or issues have been raised in the preliminary review)* and if it appears to generally meet the criteria for establishing an account at the Bank as a central bank or monetary authority, such as responsibility for:

- acting in the capacity of fiscal agent for a nation's government;
- currency issuance and/or control;
- the licensing and/or supervision of banks;
- the execution of exchange rate policies;
- the issuance of government securities;
- the operation and/or supervision of the payments system;
- establishing and executing monetary policy; and
- maintaining and managing foreign exchange reserves.

In the event that there are concerns about the legal status of the country, organization or officials, then the review must be escalated to involve Markets, International Affairs, Legal and Compliance senior management, and may extend to the Federal Reserve Board. The Treasury or State Department may also be consulted.

3. If the institution, as defined in their request or based on research findings, appears to meet any or all of the above criteria send an initial reply, outlining the general criteria for establishing such a relationship and requesting further information about the functions and responsibilities of the institution, including an official copy of the institution's establishing laws or statutes, in English

Internal FR

translation. *In addition, request information about the general purpose of the account and the institution's intended use of the account.*

4. On receipt of the establishing documentation, forward a copy to the Legal Department with a request for review to determine eligibility to establish an account at the Bank. The Legal Department will prepare a memo based on this review advising of, and explaining their recommendation in regard to, the approval of the request.
5. If Legal recognizes the Bank's authority to establish an account under the FRA, on receipt of a memo prepare a summary of their findings in an Aide Memoire, which will be reviewed and approved by a CBIAS Officer.
6. Prepare a letter to the Head of International Finance at the Board of Governors, for the signature of the CBIAS Senior Vice President, using the summarized information in the Aide Memoire.
7. On receipt of an approval letter from the Board of Governors, prepare account documents and cover letter advising of approval to establish an account and describing the account services. The letter will request a current copy of the organization's list of authorized signatories. The enclosed documents to be executed will include:
 - Account Agreement
 - Supplemental Account Agreement (Not needed if account-holder has signed 2013 version of account agreement)
 - Understanding with Regard to Authenticated Telecommunications (Not needed if account-holder has signed 2013 version of account agreement)
 - Draft Letter of Standing Instructions

Exemption 7



Internal FR

Exemption 7



11. Establish the account on the books of the FRBNY (see next section).

**ACCOUNT AGREEMENT
BETWEEN
THE FEDERAL RESERVE BANK OF NEW YORK
AND
[NAME OF ORGANIZATION]**

This Account Agreement (this “**Agreement**”), dated as of [INSERT DATE], is between the Federal Reserve Bank of New York (the “**Reserve Bank**”), a corporation organized under the laws of the United States of America with its principal office located at 33 Liberty Street, New York, New York 10045, USA, and [INSERT NAME] (the “**Account Holder**”), an entity organized under the laws of [INSERT JURISDICTION] with its principal office located at [INSERT PHYSICAL ADDRESS], and sets forth the terms and conditions that govern all accounts and account services provided by the Reserve Bank to the Account Holder. [This Agreement supersedes and replaces in its entirety the letter of terms and conditions dated as of [INSERT DATE] and the supplemental letter of terms and conditions dated as of [INSERT DATE], each between the Reserve Bank and the Account Holder.]

INTRODUCTION

The Reserve Bank provides correspondent and custodial banking services to central banks, monetary authorities, international organizations, foreign governments, and certain other official institutions in order to facilitate their official financial functions and to foster mutually beneficial relationships between the Reserve Bank and those institutions. In furtherance of this objective, the Reserve Bank and the Account Holder hereby agree as follows:

ARTICLE 1. GOVERNING DOCUMENTS

1.1. Terms of Service

The accounts and account services provided by the Reserve Bank pursuant to this Agreement will be also governed by the Terms of Service published on the Reserve Bank’s secure account-holder website (the “**Terms of Service**”), which are hereby incorporated into this Agreement by reference, as they may be amended and supplemented from time to time in accordance with Section 3.5 below. The Reserve Bank will make the current version of the Terms of Service available to the Account Holder on the Reserve Bank’s secure website, and will provide appropriate access to representatives of the Account Holder authorized to access the website in accordance with the Reserve Bank’s standard security protocols. The Reserve Bank will also provide a copy of the current version of the Terms of Service by post or electronic mail upon the Account Holder’s request. In the event of a conflict between the provisions of this Agreement and the Terms of Service, this Agreement will govern.

1.2. Other Documents

The accounts and account services provided by the Reserve Bank pursuant to this Agreement will also be subject to all applicable Reserve Bank operating circulars and

applicable regulations issued by the Board of Governors of the Federal Reserve System in accordance with their terms, including, but not limited to, Operating Circular Nos. 2, 5, 6, and 7, Subpart B of Regulation J, and Regulation N. The Account Holder acknowledges that Reserve Bank operating circulars and Federal Reserve regulations are publicly available on Federal Reserve System websites. The Reserve Bank will make reasonable efforts to provide links or other references to applicable Reserve Bank operating circulars and Federal Reserve regulations in the Terms of Service, but the absence of such a reference will not affect the applicability of this paragraph.

ARTICLE 2. ACCOUNTS

2.1. Establishment of Accounts and Related Services

Upon the Account Holder's request and at the discretion of the Reserve Bank, the Reserve Bank will establish a deposit account on its books for the receipt and payment of U.S. dollars, and/or a custody account for the safekeeping, clearing, settlement and servicing of securities or certain other financial instruments, and/or an account for the safekeeping of gold. The Account Holder may request the establishment of additional accounts from time to time, which the Reserve Bank may choose to establish in its sole discretion. The specific services to be provided by the Reserve Bank in connection with the Account Holder's accounts are described in the Terms of Service, and in connection with its use of any specific service, the Account Holder agrees to be bound by the applicable Terms of Service.

2.2. Written or Electronic Instructions or Other Communications

(a) Subject to the rights reserved in Section 3.4 below, the Account Holder authorizes the Reserve Bank to execute or otherwise act upon authorized and properly authenticated written or electronic instructions or other communications received from the Account Holder, or from other designated parties authorized by the Account Holder to issue instructions or other communications with respect to its accounts and recognized by the Reserve Bank, in accordance with the Terms of Service. The Account Holder will comply with the operational procedures and requirements that are set forth in the Terms of Service for both written and electronic communications with the Reserve Bank, including, but not limited to, those provisions relating to the use of authorized signature lists and the use of authenticated S.W.I.F.T. messaging or other authenticated communication arrangements, as applicable.

(b) The Account Holder may request the cancellation of an instruction previously sent to the Reserve Bank in accordance with the Terms of Service, provided that such cancellation instruction is received by the Reserve Bank at a time and in a manner affording the Reserve Bank a reasonable opportunity to act prior to the Reserve Bank's execution of the original instruction. Subject to Section 3.2, the Reserve Bank will make reasonable efforts to act on any cancellation instruction so received.

(c) The Account Holder's use of S.W.I.F.T. messaging or any other written or electronic communication acceptable to the Reserve Bank and properly authenticated

in accordance with the Terms of Service constitutes the Account Holder's agreement to use the S.W.I.F.T. authentication protocols then in effect or, if applicable, the other authentication procedures specified in the Terms of Service as a security procedure for the authentication of payment or other instructions. No security procedure used by the Reserve Bank to authenticate instructions or other communications is used to detect errors in the transmission or content of payment or other instructions.

(d) Any electronic instruction or other communication that is properly authenticated by the Reserve Bank in conformity with the Terms of Service, including, but not limited to, the use of the S.W.I.F.T. authentication protocols then in effect, will be binding upon the Account Holder and will have the same force and effect as a letter or other writing duly signed by a person authorized by the Account Holder to issue instructions or other communications to the Reserve Bank and authenticated by the Reserve Bank in accordance with the Terms of Service.

(e) The Account Holder will maintain its authentication protocols for S.W.I.F.T. messaging and any other security procedures relating to the authentication of the Account Holder's written or electronic communications in a secure and confidential manner. Access to any such authentication protocols or other security procedures should be restricted only to those individuals authorized by the Account Holder. If the Account Holder has reason to believe that the security or confidentiality of authentication protocols or other security procedures in its possession has been compromised, the Account Holder must notify the Reserve Bank immediately.

(f) Notwithstanding any other provision of this Agreement, the Reserve Bank is only liable for acting on an unauthorized funds transfer instruction if the Reserve Bank fails to comply with the agreed-upon security procedure used to authenticate such instruction or, when acting on such instruction, fails to act under principles of good faith as defined in Article 4A of the Uniform Commercial Code of the State of New York.

2.3. Sufficient Balances

The Reserve Bank will execute authorized and authenticated payment instructions from or on behalf of the Account Holder only to the extent that a sufficient balance in immediately available funds exists in the deposit account to be debited. Overdrafts in the Account Holder's deposit account are not permitted. Subject to and as further described in the Terms of Service, the Account Holder may be permitted to enter into intraday repurchase agreements with the Reserve Bank at the discretion of the Reserve Bank in order to facilitate clearing and settlement activity.

2.4. Nature of Transactions

The Account Holder represents, warrants and agrees that all transactions effected with respect to any of its accounts at the Reserve Bank are, and at all times will be, related to the Account Holder's official financial functions. If the Account Holder is a

central bank, the term “official financial functions” means holding assets or engaging in transactions in connection with the performance of central banking activities.

2.5. Transparency of Information

The Account Holder will not omit, delete or alter information in payment or transfer instructions sent by the Account Holder to the Reserve Bank for the purpose of avoiding detection of that information by any other financial institution in the payment or transfer process, particularly if such avoidance may appear to be in furtherance of activities such as money laundering, terrorist finance, or the avoidance of relevant sanctions.

2.6. Expenses, Charges and Minimum Uninvested Balances

(a) All charges and any necessary out-of-pocket expenses incurred in connection with the operation of the Account Holder’s accounts at the Reserve Bank will be charged to the Account Holder, in accordance with the schedule of charges listed in the Terms of Service. The Reserve Bank reserves the right to assess additional charges against any of the Account Holder’s accounts in special cases, or under circumstances in which the Reserve Bank deems such charges to be appropriate, upon prior written notice to the Account Holder.

(b) In addition, the Account Holder and the Reserve Bank will mutually agree from time to time in writing or by S.W.I.F.T. message on a suitable level for the minimum uninvested cash balance to be maintained in the Account Holder’s deposit accounts, which is intended to compensate the Reserve Bank for its day-to-day operating costs and which will be generally based on an assessment of the Account Holder’s custody holdings and transactional activity.

2.7. Security Interest

To secure any obligation, now existing or arising in the future, owed by the Account Holder to the Reserve Bank under this Agreement or any other agreement between the Account Holder and the Reserve Bank that incorporates the terms of this Agreement by reference, the Account Holder grants to the Reserve Bank a security interest in all of the Account Holder’s right, title, and interest in property, whether now owned or hereafter acquired, in the possession or control of, or maintained with, the Reserve Bank, excluding

- (i) any property that the Account Holder is prohibited from encumbering under applicable U.S. law;
- (ii) any property that the Account Holder does not have the authority to encumber under the law of the jurisdiction where the Account Holder is organized or, if applicable, the treaty under which the Account Holder is organized, provided that

the Account Holder has described to the Reserve Bank in writing the specific limitations to its authority and the property subject to such limitations, and the Reserve Bank has acknowledged such information in writing; and

- (iii) any property pledged, assigned, charged or posted as collateral by a third party to the Account Holder, or sold to the Account Holder by a third party subject to a repurchase agreement under which the Account Holder is prohibited from encumbering such property, provided that any such property is held in a segregated account on the Reserve Bank's books that the Reserve Bank has agreed will be used solely to hold such property.

Nothing in this paragraph will apply to, or grant any rights to, any third party.

2.8. Right to Recover Amounts Owed

The Reserve Bank may take any action authorized by law to recover the amount of an obligation owed by the Account Holder that is due and payable, including, but not limited to, the exercise of setoff without demand or prior notice, the realization on any available collateral pledged by the Account Holder to the Reserve Bank, and the exercise of any other rights the Reserve Bank may have as a creditor under applicable law. Nothing in this paragraph will apply to, or grant any rights to, any third party.

2.9. Tax Certification and Documentation

The Account Holder is responsible for complying with all United States tax laws relevant to its accounts at the Reserve Bank. The Account Holder will promptly submit to the Reserve Bank (a) an appropriate certification with respect to any exemption from U.S. taxation for which the Account Holder is eligible, if such a certification is not already on file with the Reserve Bank in a form acceptable to the Reserve Bank; and (b) upon the reasonable request of the Reserve Bank, any documentation deemed necessary by the Reserve Bank to comply with U.S. tax law. The Account Holder will notify the Reserve Bank promptly after it becomes aware of any event that may affect the accuracy of any certification or other documentation that has been previously submitted.

2.10. Reconciliation of Account Information

The Account Holder will promptly reconcile with its own internal records all transactional entries and balances indicated in account statements, advices or confirmations provided by the Reserve Bank, and will notify the Reserve Bank of any discrepancy in writing or by S.W.I.F.T. within thirty (30) calendar days of the day on which the relevant statement, advice or confirmation is made available to the Account Holder. All such entries and balances will be deemed correct absent any such notification, provided that the Reserve Bank will make reasonable efforts to resolve any discrepancies identified by the Account Holder subsequent to the expiration of the notice period.

ARTICLE 3. GENERAL PROVISIONS

3.1. Confidentiality

(a) The Reserve Bank will maintain the confidentiality of all information obtained in connection with the Account Holder's accounts, except that the Reserve Bank may disclose any information (i) that is required to be disclosed by law; (ii) for purposes of law enforcement or criminal investigation; (iii) to any other Federal Reserve Bank, the U.S. Department of the Treasury, or any other government or regulatory agency in the United States that has a need to know such information and that has itself agreed to maintain such information in a confidential manner; or (iv) with respect to which the Account Holder has authorized such disclosure in writing or by other authenticated communication. In addition, the Reserve Bank may disclose aggregated information to any party, as long as such disclosure does not reveal data that reasonably could be used to identify information specific to the Account Holder.

(b) For purposes of the Reserve Bank's Freedom of Information Policy, the Reserve Bank will treat confidential Account Holder records as records that are not subject to disclosure, notwithstanding any reference in such policy to the Reserve Bank's discretion to disclose information. The Reserve Bank will provide notice to the Account Holder of (i) any material changes to the Reserve Bank's Freedom of Information Policy; and (ii) any legal action brought against the Reserve Bank to compel disclosure of confidential Account Holder records, including challenges to the Reserve Bank's decision not to disclose records and the receipt of any subpoena or other legal process that does not prohibit the Reserve Bank from disclosing its existence to the Account Holder. The Reserve Bank reserves the right to decline to defend against any such legal action, but the Account Holder may petition to intervene in order to seek a protective order or other appropriate remedy in connection with such action at the Account Holder's sole expense. If the Reserve Bank declines to defend and the Account Holder does not intervene, the Reserve Bank reserves the right to disclose the information requested under such legal action.

(c) Nothing in this section will limit the ability of the Reserve Bank to disclose information to the Board of Governors of the Federal Reserve System in connection with the Board's exercise of its supervisory authority over the Reserve Bank.

3.2. Limitation of Liability

Except as may be otherwise expressly agreed upon in writing or by other authenticated communication, the Reserve Bank assumes no responsibility for any loss incurred by the Account Holder in connection with any services provided by the Reserve Bank to the Account Holder, except to the extent that such loss has been caused by a breach of the liability standards set forth in this Agreement applicable to actions taken by the Reserve Bank or any of its officers or employees or, if no such standard is specified, the negligence or intentional misconduct of the Reserve Bank or any of its officers or employees. In circumstances where the Reserve Bank is liable, the Reserve Bank's

liability will be limited to direct losses, and will not include special, incidental or consequential damages. The Reserve Bank assumes no responsibility for any delay or failure to perform an obligation that is caused by events beyond the Reserve Bank's reasonable control.

3.3. Indemnification

Except as may be otherwise expressly agreed upon in writing or by other authenticated communication, the Account Holder will indemnify and hold the Reserve Bank harmless against any claim, loss, damage, cost or expense, including but not limited to attorney's fees and the expenses of litigation, arising out of this Agreement, except to the extent that such claim, loss, damage, cost or expense has been caused by a breach of the liability standards set forth in this Agreement applicable to actions taken by the Reserve Bank or any of its officers or employees or, if no such standard is specified, the negligence or intentional misconduct of the Reserve Bank or any of its officers or employees. The Reserve Bank will give the Account Holder prompt notice of its receipt of any third-party notice or other indication of any claim, investigation or demand that might give rise to any losses required to be paid under this paragraph, but failure to provide such notice will not relieve the Account Holder of its obligations under this Agreement unless it is materially prejudiced or otherwise forfeits rights or defenses by reason of such failure. The Account Holder will have the right to conduct the defense of any third-party action for which the Reserve Bank is indemnified under this paragraph at the Account Holder's sole expense, subject to the Reserve Bank's right to participate in any such defense and to consent to any settlement or admission made on behalf of the Reserve Bank.

3.4. Reservation of Rights

(a) The Reserve Bank reserves the right at any time, upon notice to that effect, to limit the number of accounts maintained and volume of any transactions undertaken by the Reserve Bank for the Account Holder. The Reserve Bank also reserves the right to decline to offer to the Account Holder any account services listed in the Terms of Service, in the Reserve Bank's sole discretion.

(b) The Reserve Bank reserves the right to reject any written or electronic instruction received from the Account Holder that is not properly formatted or authenticated in accordance with the relevant provisions of the Terms of Service. In the event that the Reserve Bank receives conflicting instructions, the Reserve Bank will make reasonable efforts to resolve the conflict by attempting to contact the Account Holder, but reserves the right to take no action or, upon notice to the Account Holder, to take any action that the Reserve Bank determines is appropriate in its sole discretion. Except as specified in Section 3.2, the Reserve Bank will not be responsible for any delay in executing an instruction that is not received in accordance with the deadlines or proper format specified in the Terms of Service.

(c) Upon the reasonable request of the Reserve Bank, the Account Holder will provide additional information to the Reserve Bank about any instruction submitted

to the Reserve Bank or any transaction that has occurred or will occur in the Account Holder's accounts. The Reserve Bank reserves the right, in its sole discretion as exercised under principles of good faith as defined in Article 4A of the Uniform Commercial Code of the State of New York, to delay the execution of, or to decline to execute, any instruction received from or on behalf of the Account Holder, and will provide prompt notice to the Account Holder of any such delay or decision not to execute and, to the extent permitted by applicable law, the reason for such delay or decision.

(d) The Reserve Bank is required to comply with certain U.S. asset control laws, including laws that may require certain property to be blocked in connection with the enforcement of U.S. economic sanctions. In cases where blocking is not required, the Reserve Bank reserves the right, in its sole discretion, to return any funds or securities received into the Account Holder's accounts if the Reserve Bank reasonably believes that the receipt of such funds or securities is inconsistent with U.S. law. In such cases, the Reserve Bank may effect such return by originating a funds or securities transfer on the Account Holder's behalf. The Reserve Bank will promptly notify the Account Holder upon originating any such return, or upon blocking any property in accordance with applicable law.

(e) The Reserve Bank reserves the right, in its sole discretion, to debit or credit the Account Holder's deposit or securities accounts, without further authorization or instruction, solely for purposes of transferring funds or securities received into one of the Account Holder's accounts to another of the Account Holder's accounts in those cases where the Reserve Bank has received a prior communication sent by or on behalf of the Account Holder indicating an expectation to receive such funds or securities into the latter account.

(f) Because the Account Holder's transactions may affect the domestic financial markets in the United States and therefore be weighed in the course of U.S. monetary policy deliberations, the Reserve Bank reserves the right to request information from the Account Holder concerning substantial movements of its funds or securities in the United States that may not necessarily involve the Reserve Bank. The Account Holder's decision to respond to any such request will be made on a strictly voluntary basis, and any information provided by the Account Holder will be maintained in a confidential manner in accordance with Section 3.1. In some cases, the Reserve Bank may also make suggestions to the Account Holder about the timing and execution of its material United States financial transactions in order to avoid conflict with domestic monetary policy objectives.

3.5. Amendment

This Agreement may only be amended in a writing signed by authorized officials of both parties hereto; provided, however, that the Reserve Bank may amend the Terms of Service at any time, and provided further that any amendments to the Terms of Service will only become effective upon thirty (30) calendar days prior written or

electronic notice to the Account Holder, unless the Reserve Bank determines in its sole discretion that a shorter notice period is required in a particular circumstance.

3.6. Termination, Survival of Rights and Assignment

Either party may terminate this Agreement upon prior written or electronic notice to the other party. Each party will endeavor, but does not bind itself, to give the other party thirty (30) calendar days prior written or electronic notice of termination. Notwithstanding any termination of this Agreement, the rights and obligations of the parties will remain in effect with respect to transactions initiated prior to the effectiveness of such termination, until such time as those transactions are completed. The provisions of Section 3.1 regarding confidentiality and Section 3.3 regarding indemnification will survive and continue after the termination of this Agreement. Neither party will have the right to assign any rights or obligations under this Agreement without the prior written consent of the other party.

3.7. Applicable Law and Jurisdiction

(a) This Agreement and the rights and obligations described herein or arising out of this Agreement will be governed by the Federal law of the United States of America and, in the absence of controlling Federal law, in accordance with the laws of the State of New York.

(b) Any legal action, suit, or proceeding arising out of, or in connection with, this Agreement will be subject to the exclusive jurisdiction of the United States District Court for the Southern District of New York. Solely with respect to disputes between the parties to this Agreement, the Account Holder submits to the jurisdiction of such court, and waives any objection to venue or inconvenient forum with respect to proceedings brought in such court. Notwithstanding the foregoing, the Reserve Bank reserves the right to enforce this Agreement against the Account Holder in any jurisdiction in which the Account Holder maintains assets.

(c) Nothing in this Section 3.7 constitutes an explicit or implied waiver of any jurisdictional immunity to which the Account Holder may be entitled under applicable law in connection with disputes with, or claims raised by, any third party. In addition, nothing in this Section 3.7 constitutes an explicit or implied waiver of any immunity from attachment in aid of execution, or from execution, to which the Account Holder may be entitled under applicable law in connection with disputes with, or claims raised by, any party, including the Reserve Bank.

3.8. Severability and Counterparts

(a) If any provision of this Agreement is held to be invalid, illegal, or unenforceable, the remainder of this Agreement will not be affected thereby and will continue in full force and effect.

(b) This Agreement may be executed by the Account Holder and the Reserve Bank in separate counterparts, each of which will be an original and both of which taken together will constitute one and the same agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their undersigned duly authorized officers as of the date and year first above written.

**FEDERAL RESERVE BANK
OF NEW YORK**

[NAME OF ACCOUNT HOLDER]

[SIGNATURE]

[SIGNATURE]

[PRINTED NAME]

[PRINTED NAME]

[TITLE]

[TITLE]

[DATE]

[DATE]