

# First Asset Financial Inc.

## Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

---

### **1. Firm Policy**

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

While recognizing that Money Laundering vigilance is an important function of the firm, it is also realized that the nature, makeup, and location of the firm make it an unlikely target of money launderers, as per a statement by the Securities & Exchange Commission published paper.

*Resources: [NtM 02-21](#), page 5; [SIA Preliminary Guidance for Deterring Money Laundering Activity](#) ("SIA Guidance"), at pages 2-3 (Feb. 2002).*

### **2. AML Compliance Officer Designation and Duties**

*( [NtM 02-21](#), pages 3-4, 13-14)*

The firm designates Robert L. Hamman as its Anti-Money Laundering Program Compliance Officer, with full responsibility for the firm's AML program. Robert L. Hamman is qualified by experience, knowledge and training, including over 5 securities licenses and over 30 years in the securities business with the past 25 years in a management capacity. The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and arranging the annual AML audit. The AML Compliance

Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance will ensure Suspicious Activity Reports (SAR-SFs) are filed.

The firm will provide the Financial Industry Regulatory Authority (FINRA) with contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number via the CRD system on a regular basis. The firm will promptly notify NASD of any change to this information.

*Rule(s): NASD Rule 3011.*

*Resources: [NtM 02-78](#). Firms can submit their AML Compliance Officer information through FINRA's Contact System at*

*<http://www.finra.org/RegulatorySystems/FCS/index.htm>.*

### **3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions**

#### **a. FinCEN Requests Under PATRIOT Act Section 314**

*Describe your firm's procedures for FinCEN requests for information on money laundering or terrorist activity. See: [NtM 02-21](#), pages 12-14, [NASD Member Alert \(2/14/03\)](#).*

Under Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at [sys314a@fincen.treas.gov](mailto:sys314a@fincen.treas.gov), or by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as

those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

*Rules: NASD Rule 3011; Section 314 of the PATRIOT Act; 31 C.F.R. § 103.100.*

*Resources: [www.fincen.gov/314a\\_announcement021203.pdf](http://www.fincen.gov/314a_announcement021203.pdf);*

*[www.fincen.gov/314a\\_pressrelease02062003.pdf](http://www.fincen.gov/314a_pressrelease02062003.pdf); NASD Member Alert (2/14/03).*

#### **b. Sharing Information With Other Financial Institutions**

*Treasury regulations allowing information sharing among financial institutions became effective immediately on March 4, 2002. If your firm plans to share information with other financial institutions, describe your firm's procedures for such sharing. See: [NtM 02-21](#), page 13.*

We will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at [www.fincen.gov](http://www.fincen.gov). Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions *with whom we are affiliated*, and so we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records.

In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker (Southwest Securities, Inc.) for purposes of determining whether one of us will file a SAR-SF. In cases in which we file a SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may

share with the clearing broker a copy of the filed SAR-SF, unless it would be inappropriate to do so under the circumstances, such as where we filed a SAR-SF concerning the clearing broker or one of its employees.

*Rules: NASD Rule 3011; Section 314 of the PATRIOT Act; 31 C.F.R. §103.19; 31 C.F.R. § 103.110.*

*Other Resources: The notice form can be found at [http://www.fincen.gov/fi\\_infoappb.html](http://www.fincen.gov/fi_infoappb.html).*

#### **4. Checking the Office of Foreign Assets Control (“OFAC”) List**

Before opening an account that raises cause for concern we will check to ensure that a customer does not appear on Treasury’s OFAC “Specifically Designated Nationals and Blocked Persons” List (SDN List) (using the OFAC Web Site at [www.treas.gov/ofac](http://www.treas.gov/ofac), which is also available through an automated search tool on [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp)), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

#### **RESOURCES AVAILABLE:**

*Other Resources: NtM 02-21, page 6, n.24;*

*SDN List- <http://www.treas.gov/ofac/t11sdn.pdf>.*

*The OFAC Web site -- <http://www.treas.gov/ofac/t11facsc.pdf> -- contains checklists and information for securities firms to follow in checking the OFAC list. You can subscribe to receive updates at <http://www.treas.gov/press/email/subscribe.html>.*

*FINRA provides a search engine to automate OFAC list searches at <http://apps.finra.org/RulesRegulation/OFAC/1/Default.aspx>*

*Blocked Properties Reporting Form --*

*<http://www.treas.gov/offices/enforcement/ofac/legal/forms/td902250.pdf>.*

*Voluntary Form for Reporting Blocked Transactions –*

*[http://www.treas.gov/offices/enforcement/ofac/legal/forms/e\\_blockreport1.pdf](http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_blockreport1.pdf).*

*Voluntary Form for Reporting Rejected Transactions –*

*[http://www.treas.gov/offices/enforcement/ofac/legal/forms/e\\_rejectreport1.pdf](http://www.treas.gov/offices/enforcement/ofac/legal/forms/e_rejectreport1.pdf).*

## **5. Customer Identification and Verification**

For purposes of this rule, an “account” is defined as a formal relationship with a broker/dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loan and borrow activity, and the holding of securities or other assets for safekeeping or as collateral. The following are excluded from the definition of “account:” (1) an account that the broker/dealer acquires through any acquisition, merger, purchase of assets, or assumption of liabilities, and (2) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (“ERISA”).

Generally, upon opening an account, the registered representative will review a picture ID of the potential customer. This is normally a driver’s license, but other picture ID’s are acceptable. It is considered a “best practice”, but not required, that a photo copy of the ID be obtained.

In addition to the information we must collect under NASD Rules 2110 (Standards of Commercial Honor and Principles of Trade), 2310 (Recommendations to Customers - Suitability), and 3110 (Books and Records), and SEC Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented, and maintained a written Customer Identification Program (or CIP) in the FAF Compliance Manual (A Version). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information on the reverse side of the FAF “Account Form-Patriot Act Revision” and is disclosed on FAF’s website: [www.firstassetfinancial.com](http://www.firstassetfinancial.com), under “Important Information” and under the title “Customer Identification Program Notice.”

First Asset Financial Inc. is not be required to verify the identities of persons with existing accounts at the firm, as long as FAF has a reasonable belief that it knows the true identity of the customer.

### **a. Required Customer Information**

*Prior* to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office (“APO”) or Fleet Post Office (“FPO”) number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or

other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons). In the event that a customer has applied for, but has not received, a taxpayer identification number, we will accept a copy of the application to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

At this time FAF does not allow accounts to be established with foreign businesses or enterprises.

### **b. Customers Who Refuse To Provide Information**

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

### **c. Verifying Information**

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers.

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In “cleared accounts” there is a “second check” on the identity through non-documented means. Although not allowed to rely on this “second check,” by regulators, it does offer a non-documentary check of identity that is not performed by FAF. Between the two checks, the identity should be reliably confirmed.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver’s license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification in the following situations: (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when the firm is unfamiliar with the documents the customer presents for identification verification; (3) when the customer and firm do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-SF in accordance with applicable law and regulation.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body. We will identify customers that pose a heightened risk of not being properly identified.

#### **d. Lack of Verification**

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF in accordance with applicable law and regulation.

#### **e. Recordkeeping**

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

#### **f. Comparison with Government Provided Lists of Terrorists and Other Criminals**

From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time after these lists are received, we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all Federal directives issued in connection with such lists.

We will continue to comply with Treasury's Office of Foreign Asset Control rules prohibiting transactions with certain foreign countries or their nationals.

*Other Resources:* [NtM 02-21](#), page 6, n.24; 31 C.F.R. §§ 103.122.

#### **g. Notice to Customers**

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by Federal law. We will use the following method to provide notice to customers:

**Money Laundering Compliance:** FAF and the Clearing Broker are subject to laws that require FAF to attempt to prevent money laundering through FAF accounts. The signatory recognizes that FAF must verify, among other things, the identity and the source of the funds of the persons/entities signed on the front, to ensure the customer(s) is not a person, or acting on behalf of a person, that FAF and Clearing Broker are legally precluded from doing business with or that the customer's funds have not been acquired through illegitimate means. The person(s) whose signature appears on the front of this form agrees to make every reasonable effort to comply in a timely manner with any request from FAF and Clearing Broker for documents or other information concerning the signatories, the signatories' business, or the signatories' funds. The signatories recognize that FAF may refuse to open an account or may close an account if FAF is unable to verify, among other things, the signatory's identity or the source of funds.



Or:

**Important Information About Procedures for Opening a New Account**

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

**What this means for you: When you open account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.**

Rule: 31 C.F.R. §103.122(g).

**h. Reliance on Another Financial Institution for Identity Verification**

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our customer identification program with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions:

- When such reliance is reasonable under the circumstances;
- When the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h), and is regulated by a Federal functional regulator; and
- When the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the customer identification program.

*This reliance would be, specifically, in the case of investment advisory firms and our clearing broker dealer, Southwest Securities, Inc.*

**6. Foreign Correspondent Accounts and Foreign Shell Banks**

**First Asset Financial Inc. does not establish, maintain, administer, or manage correspondent accounts for unregulated foreign shell banks, as a firm's policy. All principals approving accounts shall be made aware of this and refuse approval of such accounts.**

FAF will detect correspondent accounts (any account that permits the foreign financial institution to engage in securities or futures transactions, funds transfers, or other types of financial transactions) for unregulated foreign shell banks by reviewing all new accounts

opened for titles, documentation, addresses or other evidence of shell banks or persons associated or acting for foreign shell banks. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

## **7. Private Banking Accounts/Foreign Officials**

**FAF does not permit the opening or acceptance of "private banking" accounts for non-U.S. persons. Detection of any such account will be made by account information such as name, address, CIP identification information, or other information that might be present.**

## **8. Monitoring Accounts For Suspicious Activity**

FAF will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags” identified in Section 8. b. below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed. Our monitoring of specific transactions includes: a. A daily review of all trades b. a periodic review of active clients.

### **a. Emergency Notification to the Government by Telephone**

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a

transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), U.S. Attorney's Office in Wichita, Kansas, FBI Office in Wichita, Kansas, and local SEC Office in Denver, Colorado.

#### **b. Red Flags**

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

### **c. Responding to Red Flags and Suspicious Activity**

When a member of FAF detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-SF.

## **9. Suspicious Transactions and BSA Reporting**

### **a. Filing a Form SAR-SF**

FAF will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) \$5,000 or more of funds or assets where we know, suspect, or have reason to suspect: 1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation, 2) the transaction is designed, whether through structuring or otherwise, to evade the requirements of the BSA regulations, 3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. [See: [NtM 02-21](#), page 9.] In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory

Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO. [See: [NtM 02-21](#), page 10, n.35.]

All SAR-SFs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

#### **b. Currency Transaction Reports (CTR)**

*that are customarily used and accepted as a medium of exchange in a foreign country.*

FAF prohibits the receipt of currency. If we discover currency has been received, we will file with FinCEN CTRs for transactions involving currency that exceed \$10,000. Multiple transactions will be treated as a single transaction if they total more than \$10,000 during any one business day. We will use the CTR form at [http://www.fincen.gov/reg\\_bsaforms.html#4789](http://www.fincen.gov/reg_bsaforms.html#4789).

**c. Currency and Monetary Instrument Transportation Reports (CMIR)**

Our firm prohibits the receipt of currency and has the procedures described in the previous subsection to prevent its receipt. If we discover currency has been received, we will discipline the offending party and may terminate the individual, if warranted. We will file with the Commissioner of Customs a CMIR whenever the firm transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than \$10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days) in or out of the U.S. We will file a CMIR for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the firm by means other than the postal service or common carrier, even when such shipment or transport is made by the firm to an office of the firm located outside the U.S. We will use the CMIR Form at [http://www.fincen.gov/reg\\_bsaforms.html#4790](http://www.fincen.gov/reg_bsaforms.html#4790).

**d. Foreign Bank and Financial Accounts Reports (FBAR)**

We will file with FinCEN an FBAR for any financial accounts of more than \$10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the FBAR Form at <http://www.fincen.gov/f9022-1.pdf>.

**e. Transfers of \$3,000 or More Under the Joint and Travel Rule**

When we transfer funds of \$3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of the firm (i.e., customers of the firm who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance).

**10. AML Record Keeping**

**a. SAR-SF Maintenance and Confidentiality**

FAF will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will

segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. We will share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

#### **b. Responsibility for AML Records and SAR Filing**

Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required. *See: [NtM 02-21](#), page 14.*

#### **c. Records Required**

As part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (*See* Section 5 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

*Rules: NASD Rule 3011; 31 C.F.R. §103.19; 31 C.F.R. §103.33(f).*

### **11. Clearing/Introducing Firm Relationships**

FAF will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. Both our firm and our clearing firm have filed (and kept undated) the necessary annual certifications for such information sharing, which can be found at [http://www.fincen.gov/fi\\_infoappb.html](http://www.fincen.gov/fi_infoappb.html). As a general matter, we have agreed that our clearing firm will monitor customer activity on our behalf, and we will provide our clearing firm with proper customer identification information as required to successfully monitor customer transactions. We have allocated these functions and set them forth in a written document. We understand that the allocation of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the PATRIOT Act and its implementing regulations.

*Rules: NASD Rule 3011; Sections 314(b) and 352 of the PATRIOT Act; Section 3.b. above.*

### **12. Training Programs**



We will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. Currently our training program is to include a presentation on Anti-Money Laundering in our Annual Compliance Meeting. The other method used is to include an Anti-Money Laundering unit in our "firm element of continuing education" each year to be assured that all are trained or have the opportunity to review anti-money laundering detection concepts. FAF will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

### **13. Program to Test AML Program**

#### **a. Staffing**

The testing of our AML program will be performed by management or compliance personnel of another broker dealer. Their qualifications include management experience and qualification by examination as a "Principal" or similar qualification. This is necessary, as there are no other persons within First Asset who qualifies as "independent" under the definitions under the regulations. There are three potential firms that may supply an examiner for the AML Program at First Asset:

Main Street Securities, Hays, Kansas  
Professional Investment Services, Inc., Winfield, Kansas  
Plan Professionals, Topeka, Kansas

None of the above firms are related to First Asset Financial Inc. in any way.

#### **b. Evaluation and Reporting**

After we have completed the testing, the inspector from the non-related broker dealer will report its findings to senior management. We will address each of the resulting recommendations.

### **14. Monitoring Employee Conduct and Accounts**

FAF will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual office inspection. The AML Compliance Officer's accounts will be reviewed by David Fanshier.

## **15. Confidential Reporting of AML Non-Compliance**

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to Thaine Streit. Such reports will be confidential, and the employee will suffer no retaliation for making them.

## **16. Additional Areas of Risk**

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. There are no major areas at this time, but should they arise, they will be added under this section.

## **17. Senior Manager Approval**

I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Signed:

Robert L. Hamman

Title: President

Date: \_\_\_\_\_

**8/16/07**

**Please note:** The Financial Crimes Enforcement Network has issued final rules to implement requirements set forth in Sections 311 and 312 of the USA PATRIOT Act, which have not yet been incorporated into the template. These rules include 31 CFR 103.176, 31 CFR 103.188, 31 CFR 103.192, and 31 CFR 103.193. This booklet does not reflect these recent changes.