AML For Futures Brokers

To complete this training simply follow these instructions:

1. Read all the way through the text on this page.
2. At the very end of the page, there will be a blue button labeled “Sworn Declaration”. Click on the button.
3. Fill out the form carefully. Your certificate will be sent to the email you put in.
4. Click the button that says “Submit”.
5. If you are with either Americash or United Fidelity Funding Corp, click the button that matches. Otherwise click the button labeled “Click here to pay by credit card”.
6. Select the course that you completed from the list by clicking “Add to cart”.
7. Once the item has been added, a popup will show at near the top right, click the button that says “Checkout”.
8. Click the button that says “Checkout”.
9. Fill out your information and credit card information for processing.
10. Once payment has been received, we will send your certificate to the email you put in the form.

To scroll this course, move your mouse pointer to the arrow at the bottom of the vertical, narrow scroll bar on the right. Left click the mouse and scroll. On the last page, click Sworn Declaration, print, complete and send to us.

The Walsh Agency designed this newly streamlined AML compliance course to be as law abiding and as user-friendly as possible. Our research to develop this course included our in-person interviews with the CFTC’s AML Staff in Washington, D.C. and the NFA’s AML Staff in Chicago. It also incorporates ideas for ease-of-use features we’ve received over the years from our clients: APs, IBs, FCMs, brokers and compliance and registration officers.

This course uses EZ Scroll navigation. No timers. No tests. No clocks. Take at your pace. If you have questions, please call our 24/7/365 days live help line: (410) 207-0134. On the last page of this course, click on the link to your Sworn Declaration. Print it, fill it out and send it us. We’ll certify you and send your Certificate, good for one year, within three business days.

Dear Reader,

Please consider for a moment, the importance of this course to help prevent money laundering and terrorist financing.

Just think of the serious consequences to yourself, your career and your company, if even one of your clients was found guilty of using you and your firm for money laundering and terrorist financing.

It is critical you take this AML compliance training requirement seriously.

Sincerely, John Walsh, for the Walsh Agency, Inc.

Introduction

You are required to follow all laws and rules pertaining to Anti-Money Laundering Procedures as outlined in the US Patriot Act, the guidance found in NFA’s Compliance Rule 2-9(c) and NFA’s Interpretive Notice 9045. Those requirements are included in this course.

An important component of this rule is the requirement that FCM and IB members provide on-going education and training, such as this course, for all appropriate personnel.

This course also contains transcriptions of the Commodity Futures Trading Commission’s Anti-Money Laundering rules and regulations. It includes a substantial amount of material from the National Futures Association’s Anti-Money Laundering Interpretive Notice 9045.

Therefore, by necessity, some content is duplicated.

AML Compliance is a Federal Regulation.

Your obligation to comply with an Anti-Money Laundering Program and take Anti-Money Laundering compliance training is a regulation of the Federal Government.

The USA Patriot Act amended the Bank Secrecy Act and established the AML rules and regulations developed and written by:

- The Department of the Treasury.
- The Financial Crimes Enforcement Network (FinCEN).
- The Commodity Futures Trading Commission (CFTC).

The CFTC’s directive on Anti-Money Laundering and Terrorist Financing:

The Patriot Act, which amends the Bank Secrecy Act (BSA), was adopted in response to the September 11th terrorist attacks.

The Patriot Act is intended to strengthen U.S. measures to prevent, detect and prosecute international money laundering and the financing of terrorism. These efforts include new anti-money laundering (AML) tools that impact the banking, financial and investment communities.

Under the Patriot Act, associated persons who are, or are required to be, registered including: futures commission merchants (FCMs) and introducing brokers (IBs) are subject to new requirements for establishing AML Programs, which include verifying the identity of customers, dealing with certain types of accounts involving foreign persons and reporting suspicious activity.

AML Compliance Training Programs must be ‘firm specific’.

The National Futures Association requires AML Compliance Training to be ‘firm specific’ and that ‘one size does not fit all’.

NFA’s guidelines for members regarding AML compliance training regulations state…“AML Programs will vary depending on a member’s type of business, the size and complexity of its operations, the breadth and scope of its customer base, the number of firm employees and the firm’s resources.” (From the NFA’s AML Interpretive Notice 9045)

To further quote from NFA’s Interpretive Notice 9045: “This training program shall include: 1. annual training on their firm’s AML policies and procedures. (GIBs can meet that requirement by reading and understanding their FCM’s AML Policies and Procedures.) The training program shall also include: 2. the relevant federal laws and NFA’s guidance issued in this area.” This training fulfills #2. of the requirement. Therefore, in addition to this course material, you must read, understand and comply with your firm’s AML Policies, Procedures and Controls.

Overview

1. Provider
2. Instructor
3. Course description
4. ‘Take a break’ from this course and return
5. Sworn Declaration (SD) Worksheet and Invoice
6. Certification and your Professional AML Certificate – suitable for framing
7. Free tutorial ***How To Sell Futures***

Provider

The Walsh Agency Inc., a Connecticut Corporation founded in 1970, has been helping brokers sell futures since 1976. We have conducted sales and trading classes and, as they became required, Ethics Training and Anti-Money Laundering Courses for more than 20,000 futures professionals. Home office employees and brokers (APs) from several FCMs and IBs have taken one or more of our courses, including: ADMIS, Crossland, Dorman, FC Stone, LPL Financial, Merrill Lynch, PFG, Penson, Prudential Financial, RCG, R.J. O’Brien and Vision.

The Walsh Agency, Inc. is proud to be one of the earliest members of the Association of Certified Anti-Money Laundering Specialists (2004).

Instructor

John Walsh has worked with futures professionals for over thirty-five years. In 2004, he earned the designation of Certified Anti-Money Laundering Specialist (CAMS). In this AML Course, he shows you what you need to do to comply with the federal government’s AML regulations as written by the Department of Treasury, Financial Crimes Enforcement Network (FinCEN), the Commodity Futures Trading Commission (CFTC), implemented by the National Futures Association (NFA) as well as your firm’s AML Policies, Procedures and Controls.

John has written several books about futures including: ***Ethics Training for Futures Professionals, How to Trade Futures, How to Sell Futures, How to Raise Managed Money for Commodity Trading Advisors (CTAs) and Commodity Pool Operators (CPOs) including Funds*** and ***Master Brokers,*** interviews with top futures brokers. He’s also written booklets, brochures and courses such as: ***Anti-Money Laundering Compliance for Futures Professionals, Why most Futures Traders Lose Money, Basic Training for Futures Traders, Advanced Training for Futures Traders*** and ***Introduction to Financial Futures.***

Course Description

We designed our AML training to teach registrants the rules and regulations to help keep themselves, their supervisors and the officers and owners of their companies well within the regulations and out of trouble. To make sure our AML Compliance Training Course contains the best information to meet these objectives, before we compiled this course we:

- Interviewed AML personnel at the Financial Crimes Enforcement Network (FinCEN).
- Conducted in-person interviews with the Commodity Futures Trading Commission’s (CFTC’s) AML staff in Washington, D.C.
- Conducted in-person interviews with the National Futures Association’s (NFA’s) AML staff in Chicago, Illinois.
- Conducted in-person interviews with Compliance Officers of FCMs who have a substantial presence in the Introducing Broker Community.
- Studied the Anti-money Laundering laws, rules, regulations and the National Futures Association’s AML Interpretive Notices and Guidelines.

Everything in this AML Compliance Training Course is based on facts.

Our course material comes from our interviews and the following sources:

1. Final Rule for Customer Identification Programs (CIP) Federal Register.
2. Final Rule for Suspicious Activity Reports (SARs) Federal Register.
3. The CFTC's AML Compliance Guidelines.
4. The CFTC's Q and A report on Customer Identification Programs.
5. The National Futures Association's (NFA) AML Compliance Rule 2-9(c).
6. The NFA's Interpretive Notice 9045: AML Programs.
7. The NFA's annual AML Compliance Questionnaire for FCMs and IBs.
8. The NASD's AML Template: Compliance and Supervisory Procedures.
9. The Securities Industry Association's AML Compliance Guidelines.
10. Financial Crimes Enforcement Network (FinCEN).
11. Office of Foreign Assets Control (OFAC).
12. Financial Action Task Force on Money Laundering (FATF).
13. Investment Reference Company – an Independent Firm that audits IBs.
14. The USA Patriot Act.
15. The Bank Secrecy Act (BSA).
16. The Department of the Treasury.
17. IOSCO – International Organization of Securities Commissions.
18. The Association of Certified Anti-Money Laundering Specialists.

This AML course is divided into four sections:

Section 1 – AML Rules and Regulations
Section 2 – Customer Identification Programs Part A
Section 3 – Customer Identification Programs Part B
Section 4 – Suspicious Activity Reports (SARs), Audits and the NFA's Annual AML Questionnaire

This AML course includes the following topics:

1. Federal Government's AML Rules and Regulations
2. The development of Internal AML Policies and Procedures
3. The designation of an AML Compliance Officer
4. An on-going employee AML Training Program
5. An independent audit function to test the AML program
6. Customer Identification Program (CIP)
7. Implementing written CIP Guidelines
8. Checking government lists for terrorists and suspects
9. Notification of customers of identification requirements
10. Record keeping and retention
11. Suspicious Activity Reports (SARs)
12. SARs filing guidelines and requirements
13. CIP red flags
14. SAR red flags
15. National Futures Association's Annual AML Questionnaire
16. National Futures Association's AML Interpretive Notice 9045

Those sixteen topics are listed on your AML Certification Document.

'Take a break' from this course and return

You may easily navigate quickly through this course. Each page is numbered. If you want to take a break, you're welcome to do so. Just make a note of the page where you left off and return to it at your convenience.

Sworn Declaration (SD) Worksheet and Invoice

This is the document you'll print at the end of the course. Fill in the information requested. The invoice is in the lower right hand corner of this Sworn Declaration Worksheet.

You may email, fax or snail mail the SD to us. You'll be able to print it at the end of this course. If you don't have a printer, use any other computer with a printer, surf to this course, scroll to the last page, click on the Sworn Declaration link and print a copy.

Be sure to keep a copy of your Sworn Declaration Worksheet and your Certificate of Compliance in your files, as required, for your firm, your FCM, for your records and in the event of an audit.

Certification and your Professional AML Certificate – suitable for framing

Upon receiving your completed Sworn Declaration Worksheet and payment, we certify you and send you a copy of your AML Certificate which is suitable for framing. Many brokers do frame them and display them in their offices.

Each certificate lists the sixteen key subjects we cover in this material. It also includes the date you were certified. This date serves as a reminder of when you're required to renew your annual AML training. The Certificate, **not your Sworn Declaration**, is your proof to your company and auditors that you completed this course. Be sure to keep a copy of your Certificate of Compliance and your Sworn Declaration Worksheet in your files, as required, for your firm, your FCM, for your records and in the event of an audit. To replace a lost certificate, click the link on the last page, print and send it to us.

Free Tutorial *How To Sell Futures*

The price of this AML training includes a free copy of ***How To Sell Futures.*** It's available for printing and/or reading at the end of this course. This is an excellent guide for new brokers and for more experienced brokers who would like a refresher course on how to build their business.

For over thirty-five years, we've surveyed thousands of prospects and traders by: phone, focus groups, email, snail mail, in-person and with questionnaires at seminars. We also surveyed hundreds of successful brokers and asked them how they built their businesses. Many are in our book ***Master Brokers***, interviews with top futures brokers. This research was supervised by the Walsh Agency over several years. Cost of $200,000+ was paid for by the CME, KCBOT, NYBOT (now ICE) and several major FCMs.

We asked these prospects why they opened accounts (or why not). We asked them why they selected one firm over another. We show you what they told us about 'the main barrier to the sale' (lack of trust). We show you how top brokers overcome this number one barrier on their first contact.

The findings of this research indicate the typical broker opens one retail spec account for every ten leads. Median account opens for about $6,000. These accounts usually last about four months.

The price of this AML training includes a free copy of It's available for printing and/or reading at the end of this course. This is an excellent guide for new brokers and for more experienced brokers who would like a refresher course on how to build their business.
For over thirty-five years, we've surveyed thousands of prospects and traders by: phone, focus groups, email, snail mail, in-person and with questionnaires at seminars. We also surveyed hundreds of successful brokers and asked them how they built their businesses. Many are in our book , interviews with top futures brokers. This research was supervised by the Walsh Agency over several years. Cost of $200,000+ was paid for by the CME, KCBOT, NYBOT (now ICE) and several major FCMs.
We asked these prospects why they opened accounts (or why not). We asked them why they selected one firm over another. We show you what they told us about 'the main barrier to the sale' (lack of trust). We show you how top brokers overcome this number one barrier on their first contact.
The findings of this research indicate the typical broker opens one retail spec account for every ten leads. Median account opens for about $6,000. These accounts usually last about four months. shows brokers effective methods to open at least three larger accounts for every ten leads, increase initial deposits and trading life. also includes proven sales techniques for raising Managed Money and selling Futures Funds. ***How To Sell Futures*** shows brokers effective methods to open at least three larger accounts for every ten leads, increase initial deposits and trading life. ***How To Sell Futures*** also includes proven sales techniques for raising Managed Money and selling Futures Funds.

AML Rules and Regulations

Money Laundering Defined

Money laundering is the act of moving illegally obtained assets through the financial system to disguise their origin and make them appear legitimate.

Money Laundering occurs in three stages.

1. Placement: may involve depositing cash in small amounts into a bank. It also can consist of introducing illegally derived assets into such businesses as financial institutions, casinos, race tracks or by purchasing monetary instruments such as money orders, or by buying high value goods, for example: precious metals (gold), automobiles or insurance.
2. Layering: this phase is the movement of funds in an effort to further disguise the audit trail and ownership of funds. In this stage, assets that have been 'placed' are liquidated and transferred to other vehicles such as brokerage accounts, additional bank accounts (deposits from re-sale of high value goods) and real estate. FCMs and IBs are most vulnerable to money laundering violations in this stage. Clients can open accounts, trade with little risk, close, cash out and receive laundered funds from the brokerage firm.
3. Integration: to further obscure their source, the assets are again converted (real estate, etc.) to give the appearance of legitimacy.

Federal Regulations – Minimum Requirements

Subtitle B – Bank Secrecy Act: Amendments and Related Improvements

USA Patriot Act Amendments – Section 352 AML Programs:

In General – Section 5318(h) of title 31, United States Code, is amended to read as follows, Anti-money laundering programs:

In General – In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs, including, at a minimum:

- The development of internal policies, procedures and controls.
- The designation of a compliance officer.
- An on-going employee training program.
- An independent audit function to test the program.

Federal Regulations – (A) Policies

1. You are required to fully comply with all laws and regulations regarding money laundering.
2. You are not to be used to facilitate money laundering or the funding of terrorist or criminal activities.
3. All employees have a responsibility to follow the firm's written anti-money laundering procedures and controls and to abide by all applicable AML laws and regulations.
4. Your firm's AML policy statement should also discuss the consequences (including possible dismissal) for those who do not follow all AML rules. Penalties for conducting transactions with prohibited individuals or entities include civil penalties of up to $250,000 per violation, fines as high as $1,000,000 and/or jail sentences of up to twelve years.

Federal Regulations – (A) Procedures and Controls

Your firm's AML Procedures and Controls must cover the following:

- Your firm's AML Procedures and Controls should instruct and enable employees to follow a thorough Customer Identification Program (CIP) as outlined in the CIP regulations. (Sections 2 and 3 of this Course)
- Your firm's AML Procedures and Controls should instruct and enable employees to understand a Suspicious Activity Report (SAR) Program as outlined in the SARs regulations. (Section 4 of this Course)

Federal Regulations – (B) Designation of a Compliance Officer

The IB must designate a Compliance Officer whose duties must include, but not be limited to:

- Receiving reports of suspicious activity from firm personnel
- Gathering all relevant information to evaluate and investigate suspicious activity
- Determining whether the activity warrants reporting to the Compliance Officer of the IB's FCM
- Ensuring that all required information is recorded, maintained and retained in accordance with the regulations
- Ensuring (when appropriate) that Suspicious Activity Reports are filed in consultation the FCM's Compliance Officer

Federal Regulations – (C) On-going employee training programs

Another important component of the AML regulations is the requirement that firms provide on-going education and training for all appropriate personnel. Here is an example from the NASD's AML template for small firms (i.e. IBs).

- We will develop on-going employee training under the leadership of the AML Compliance Officer and Senior Management. Our training will occur at least once a year. It will be based on our firm's size, our customer base, our resources and our allocation agreements with our FCM."
- "Our AML 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
  - Employees' roles in the firm's AML efforts and how to perform them
  - The firm's record gathering and retention policy
  - The disciplinary consequences (including civil and criminal penalties) for non-compliance with the Patriot Act's AML rules and regulations.
  - We will require new employees to take AML training within x (sic) number of weeks of being hired.
  - We will maintain records of our annual AML audit to indicate the trainer, attendees, dates, attestations and a copy of the training matter."

Federal Regulations – (D) Independent audit function to test programs

An IB is required to provide for annual independent testing of the adequacy of its anti-money laundering program. IBs may satisfy this requirement with their personnel who are independent of the personnel working in the areas exposed to potential money laundering or by hiring an outside party with experience with this type of auditing. In either circumstance, the audit function should test all affected areas to ensure that personnel understand and are complying with the anti-money laundering policies and procedures and that these policies and procedures meet all the necessary requirements.

The results of any audit should be documented and reported to the firm's senior management or an internal audit committee or department. Follow up should be done to ensure any deficiencies in the firm's anti-money laundering program are addressed and corrected.

The audit personnel should not have AML duties and responsibilities, nor should they have a reporting relationship to the AML Compliance Officer.

The audit function and process are explained in Section Four of this Course.

You have completed Section 1: AML Rules and Regulations

As you can see, the regulators take your Anti-Money Laundering responsibilities seriously. Your effort and vigilance in creating and implementing an Anti-Money Laundering Program is an important part of the government's efforts to prevent money laundering and terrorist financing.

You may never know if you deterred any money laundering and/or terrorist financing schemes by complying with your AML program. But you will know you are doing your part in a National effort to implement the USA Patriot Act.

Customer Identification Programs Part A

CIPs for FCMs and IBs – minimum requirements

Joint final rule by: FinCEN, the Treasury and the CFTC.

To summarize the government regulations: in general, each IB must implement a written Customer Identification Program (CIP) appropriate for its size and business that, at a minimum, includes these requirements:

1. Implementing written CIP guidelines.
2. Customer identification and verification procedures.
3. Record keeping and retention procedures.
4. Checking government lists for terrorists and suspected terrorists.
5. Notifying customers of identity verification requirements.
   (4. and 5. may be may be conducted by the FCM via a written allocation agreement with the IB.)

I. Implementing written CIP guidelines

The Introducing Broker's CIP guidelines must be part of the IB's overall written Anti-Money Laundering Program.

II. (a) Customer identification and verification procedures

The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the IB to form a reasonable belief it knows the true identity of the customer.

The procedures must be based on the IB's assessment of the relevant risks, including those presented by the types of accounts maintained, the methods of opening accounts, the types of identifying information available and the IB's size, location and customer base.

II. (b) Customer information required

From individuals – U.S. Citizens. The CIP must include procedures for opening an account that specify identifying information that will be obtained from each customer:

1. Name
2. Date of birth, for an individual
3. Address, which shall be:
   - for an individual, a residential or business street address.
   - for an individual who does not have a residential or business street address, an Army Post Office (APO) box number, Fleet Post Office (FPO) box number or the residential or business street address of next of kin or another contact individual.
   - for a person other than an individual (such as a corporation, partnership or trust), a principal place of business, local office or other physical location.
4. Social security number or taxpayer identification number (TIN).
5. Investment experience and objective.
6. Net worth, liquid net worth and annual income.
7. Citizenship status (e.g. U.S. citizen, resident alien with nationality, non-resident alien).
8. Occupation, employer, employer's physical address and nature of the customer's employment/business.

For a non-U.S. person, the same information is required as in the previous list (1 through 8 for individual, U.S. citizens) and one or more of the following:

1.) A taxpayer identification number (TIN).
2. A passport number and country of issuance.
3. An alien identification card number or,
4. The number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

When opening an account for a foreign business or enterprise that does not have an identification number, the FCM or IB must request alternative government-issued documentation certifying its existence.

Correspondent accounts include accounts for foreign financial institutions to engage in futures or commodity options transactions, funds transfers, or other financial transactions, whether for the financial institution or principal or for its customers. An account includes any formal relationship established by an FCM to provide regular services, including but not limited to, those established to effect transactions in contracts of sale of a commodity for future delivery, options on a commodity or options on futures.

Customer information required from companies, trusts, partnerships or other legal entities located in the U.S.

The CIP must include procedures for opening an account that specify the identifying information to be obtained from each entity:

1. Full name and physical address of the entity (post office box, other mail drop addresses, hotels, etc. are not permitted).
2. The jurisdiction of formation and legal form of entity.
3. Taxpayer identification number (TIN).
4. Investment experience and objective.
5. The names of all persons with responsibility for the management of the affairs of the entity (directors, general partners, trustees, authorized signatories) or a copy of its annual report.
6. Copy of documents proving the existence of the entity (e.g. certificate of incorporation, memorandum and articles of association, trust deed, partnership agreement).
7. On a case-by-case basis, current list of authorized signatories or copies of powers of attorney to establish and document that the representative(s) of the entity is authorized to act on his behalf (and copies of valid government issued photo identification for all representatives). For off-shore corporate accounts and accounts for trusts established in foreign jurisdictions sufficient documentation to identify principal ownership.

II. (c) Verification through documents

For an FCM or IB relying on documents, the CIP must contain procedures that set forth the documents the FCM or IB will use. These documents may include:

- for an individual, a government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport, and;
- for a person, other than an individual (such as a corporation, partnership or trust), 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.

II. (d) Verification through non-documentary methods

According to Concord EFS, a major processor of credit card transactions in Memphis, Tennessee, there are more than 700,000 cases of identity theft in the U.S. each year resulting in losses of over two billion dollars. You may want to use non-documentary methods to attempt to verify the identity of a customer who provided you with documents you feel or believe may not be valid.

For an FCM or IB relying on non-documentary methods, the CIP must contain procedures that set forth the non-documentary methods they will use.

These may include:

1. contacting the customer;
2. independently verifying the customer's identity through the comparison of information provided by the customer with information provided from a consumer reporting agency, public database or other source;
3. checking references with other financial institutions or;
4. obtaining a financial statement.

II. (e) Verification through non-documentary methods

The FCM's or IB's non-documentary procedures must address situations when an individual is:

1. unable to present an unexpired government-issued identification
2. document that bears a photograph or other similar safeguard;
3. the FCM or IB is not familiar with the documents presented;
4. the account is opened without obtaining documents;
5. the customer opens the account without appearing in person at the FCM or IB, and;
6. where the FCM or IB is otherwise presented with circumstances that increase the risk that you will be unable to verify the true identity of a customer through documents.

II. (f) Additional verification for certain customers

The CIP must address situations where, based on the FCM's or IB's risk assessment of a new account opened by a customer that is not an individual, the FCM or IB will obtain information about individuals with authority or control of such an account in order to verify the customer's identity.

This verification method applies only when the FCM or IB cannot verify the customer's true identity after using the verification methods previously described in this section.

II. (g) Lack of verification

The CIP must include procedures for responding to circumstances in which the FCM or IB cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:

1. when the account should not be opened;
2. the terms under which a customer may conduct transactions while the FCM or IB attempts to verify the customer's identity;
3. when an account should be closed after attempts to verify the customer's identity have failed;
4. and when the FCM or IB should file a Suspicious Activity Report (SAR-SF) in accordance with the applicable laws and regulations.

III. (a) Record keeping

The CIP must include procedures for making and maintaining a record of all information obtained under the procedures covered in this section.

III. (b) Required records

At a minimum, all records must include:

1. all identifying information about a customer obtained as outlined in this section;
2. a description of any document that was relied on in this section, noting the type of document, any identification number(s) contained in the document and the place of issuance (if indicated);
3. the date of issuance and the expiration date;
4. a description of the methods and the results of any measures undertaken to verify the identity of a customer as detailed in this section;
5. and a description of the resolution of each substantive discrepancy discovered when verifying the identity information obtained.

III. (c) Retention of records

Customer identification information collected must be retained for five years after the account is closed. All other information, including a copy or description of verifying documents, a description of non-documentary methods, and a description/resolution of discrepancy must be retained for five years after the record is made.

IV. Comparison with government lists

The CIP Rule states: "The Federal Government's joint final CIP rule provides that: an FCM's or IB's CIP must include procedures for determining whether a customer appears on any lists of known or suspected terrorists issued by any Federal Agency and designated as such by the Treasury in consultation with federal functional regulators."

The Treasury and the CFTC have modified the proposed rule to provide that the CIP's procedures must require the FCM or IB to determine whether a customer appears on a list 'within a reasonable period of time' after the account is opened, or earlier, if required by another Federal law or regulation or by a federal directive issued in connection with the applicable list.

The final rule also requires an FCM's or IB's CIP to include procedures that require the firm to follow all federal directives issued in connection with such lists. Again, because no lists have yet been designated under this provision, the final rule cannot provide more guidance in this area.

This is not to say, however, that FCMs and IBs do not have obligations under the law to screen their customers against government lists. For example, FCMs and IBs should have AML compliance Programs in place to ensure they comply with OFAC's rules.

An FCM or IB member of the NFA would violate CFTC Rule 2-30, however, if it allowed a natural person to transact business before obtaining specific information about the individual's true identity.

Moreover, an FCM or IB must also comply with the Treasury's Office of Foreign Assets Control's (OFAC) regulations prohibiting transactions involving designated foreign countries or their nationals.

The final CIP rule acknowledges that there may be circumstances in which a firm may be able to rely on the performance of another financial institution (i.e. an IB relying on its FCM) for some or all of the elements of a firm's CIP.

V. Customer Notice

The CIP must include procedures for providing customers with adequate notice the FCM/IB is required to request identity verification information.

V. (a) Adequate Customer Notice

Notice is adequate if the FCM or IB generally describes the identification requirements of this section and provides such notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account. For example, depending upon the manner in which the account is opened, an FCM or IB may post a notice in its lobby or on its web site, include the notice on its account applications or use any other form of written or oral notice.

V. (b) Sample Customer Notice

An FCM or IB may use this sample language to provide notice:

"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 an account, we will ask you 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."

Customer Identification Programs Part B

Reliance on another financial institution

The government's Customer Identification (CIP) rule acknowledges there may be circumstances in which a firm may be able to rely on the performance of another financial institution (i.e., an IB relying on its FCM) for some or all of the elements of a firm's CIP. To quote from the rule:

"The CIP may include procedures specifying when the futures commission merchant or introducing broker will rely on the performance by another financial institution (including an affiliate) of any procedures of its CIP, with respect to any customer of the futures commission merchant or introducing broker that it 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 provided that:

1. such reliance must be reasonable, under the circumstances.
2. Government AML rules must apply to the other financial institution.
3. The other financial institution enters into a contract requiring it to certify annually to the futures commission merchant or introducing broker that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the FCM's or IB's CIP."

"An example of an agent relationship would be an outside vendor checking OFAC's list for an FCM or IB."

Following the government's AML regulations: "NFA Compliance Rule 2-9 (c) requires both FCMs and IBs to establish and implement anti-money laundering compliance programs and each such member has an independent customer identification and verification obligation. The NFA believes, however, that the interests of business efficiency and anti-money laundering effectiveness may best be served if FCMs and IBs cooperate with each other in order to meet their respective obligations."

From the NFA's AML Interpretive Notice 9045:

Allocation of FCM and IB AML responsibilities

The NFA Guidelines continue: "An FCM and IB may allocate between themselves, certain elements of their customer identification and verification procedures. For example, an IB may agree to use its direct relationship with the customer to obtain customer identification information and documentation, while an FCM may agree to use its automated systems to fulfill certain verification functions, such as checking customer' names and addresses against government generated lists."

"Any such allocation agreement must be clearly set forth in writing, and the FCM and IB must have a reasonable basis for believing that the other party is performing its required function. However, the Treasury takes the position that any such allocation does not relieve either the FCM or the IB from its independent obligation to comply with applicable customer identification and verification rules or other applicable AML rules."

Know your customer

NFA's 'Know your customer' Rule 2-30 applies to individuals and requires you to obtain sufficient information to provide adequate risk disclosure. The less experienced the investor, the more risk disclosure he or she may need.

NFA's 'Know your customer' AML, Rule 2-9 (c) applies to all accounts and requires you to identify and verify with whom you are doing business to attempt to determine if there is any possible money laundering or terrorist financing risk or other violations of AML rules and regulations.

Intermediated Accounts

Here are the NFA's comments from their AML Interpretive Notice 9045:

"As per the government regulations, an FCM may carry and an IB may introduce accounts for other intermediated accounts, such as omnibus accounts and accounts for commodity pools and other collective investment vehicles."

"Traditionally, with respect to such intermediated accounts, the FCM and IB would be responsible for a risk-based analysis of the money-laundering risks posed by the intermediary and the pool or other collective vehicles. In most instances, this risk-based analysis will result in the FCM or IB not having to conduct due diligence with respect to the underlying participants or beneficiaries."

"For an omnibus account where the intermediary is the account holder, the FCM should treat the intermediary as the customer and does not have to apply its CIP requirements to the underlying beneficiaries."

"If an intermediary opens an account in the name of a collective investment vehicle such as a commodity pool, the FCM or IB is not required to apply its CIP to the pool's underlying participants."

Your local customers, whom you know personally and see face-to-face, are obviously going to be easier to identify and verify than those whom you don't know or see. Our electronic age and accompanying anonymity make the detection of money laundering and terrorist financing difficult but not impossible.

Our research indicates that most retail futures accounts are prospected and opened without a personal meeting. In these days of impersonal technological communications, most accounts are now opened without anyone at the FCM or IB ever seeing the customer. That's what makes your job so challenging. But you have assistance from your IB's compliance officer and, of course, the compliance officer of your FCM.

Summary

The CIP rule, at a minimum, requires FCMs and IBs to: implement reasonable written procedures to verify the identity of any entity seeking to open an account, and to the extent reasonable and practicable, maintain records of the information used to verify the entity's identity, and determine whether the entity appears on any lists of known or suspected terrorists or terrorist organizations provided to futures commission merchants or introducing brokers by an appropriate government agency and notify customers of the requirement to confirm their identification. In a give-up arrangement, the clearing FCM, not an FCM acting solely as an executing broker, is required to apply its CIP to the customer.

The CIP rule applies to all FCMs and IBs except FCMs and IBs that register with the CFTC solely because they effect transactions in security futures products.

Red Flags – CIP

As you conduct your CIP, here is a list of customers' behaviors and/or situations designed to help you identify potential money launderers.

This list of SAR Red Flags is based on material from: the Commodity Futures Trading Commission, Financial Crimes Enforcement Network, National Association of Securities Dealers, National Futures Association, Securities Industry Association and several FCM and IB compliance officers.

1. The customer exhibits unusual concern for secrecy, particularly with respect to his/her identity or background, or refuses to complete, in its entirety, the account documentation.
2. The customer exhibits unusual concern regarding compliance with government reporting requirements, particularly with respect to his/her identity, type of business and assets.
3. Upon request, the customer refuses to identify or fails to indicate a legitimate source for his/her funds and other assets or identifies a source that is fictitious, false, misleading or substantially incorrect.
4. The customer appears to operate as an agent for an undisclosed principal but is reluctant to provide information regarding the principal or the nature of their relationship.
5. The customer is reluctant to provide complete information regarding the purpose of his/her business, banking relationships, an entity's officers and directors or location.
6. The customer has difficulty describing the nature of his business.
7. The customer lacks general knowledge of his/her industry.
8. The customer presents unusual or suspicious identification documents that cannot be readily identified.
9. For no apparent reason, the customer requests multiple accounts under a single name or multiple names.
10. The customer is from, or maintains accounts in, a country identified as a haven for money laundering, bank secrecy or narcotics production.
11. The customer, or a person associated with the customer, has a questionable background (including prior criminal convictions) or is the subject of news reports indicating possible, criminal, civil or regulatory violations.
12. The customer appeared 'out of the blue' (had not been solicited and/or opened the account with the 'broker of the day').
13. The information provided by the customer as to the source of his/her funds is fictitious, false, misleading and/or substantially incorrect.
14. The initial deposit is from a third party.
15. The customer seems unusually interested in how fast he can access his funds.
16. A customer indicates he/she is interested in engaging in a trading strategy that makes no business sense, has little or no risk and/or is not consistent with his or her stated reason for trading futures.
17. Customer exhibits a lack of concern for risk, commissions and fees.
18. The customer attempts to deposit cash, even after being told the company has a strict policy of not accepting cash.
19. The customer appears anxious or nervous when opening the account.
20. The customer opens the account via the internet, phone or mail and seems evasive about his identity, business, reasons for opening the account and other normally disclosed information.
21. The customer is a foreign Politically Exposed Person (PEP), a senior foreign government official or a family member or associate of same.

That's the end of this list. If you know of any CIP Red Flags that are not on this list, we would appreciate it if you would tell us about them. Reason? So we may include them, if appropriate, in our next periodic update of this course.

Please email any suggestions to: WalshAMLEthics@gmail.com. Please write CIP Red Flag in the subject line of the email. Thank you.

The CFTC and the NFA say Associated Persons are most likely in the best position to conduct a risk-based analysis of customer identification information, verification and documentation.

The prevention of money laundering and terrorist financing in our industry often starts with the Introducing Broker, the person on the front line. You usually have the first contact with the customer. You are a gatekeeper.

Suspicious Activity Reports (SARs), Audits and the NFA's annual AML Questionnaire

The Federal Suspicious Activity Reports (SARs) Rule:

Every Futures Commission Merchant and Introducing Broker in commodities (IB-C) within the United States shall file with the Financial Crimes Enforcement Network a report (SAR) of any suspicious transaction relevant to a possible violation of law or regulation.

The law states only one SAR is to be filed per transaction. The FCM and the IB do not both have to file.

NFA's Interpretive Notice 9045 – SARs filing guidelines

The government's SARs rules require FCMs and IBs to report suspicious transactions that are: conducted or attempted by, at, or through an FCM or IB, involve an aggregate of at least $5,000 in funds or other assets (not limited to currency) and the FCM or IB knows, suspects or has reason to suspect the transaction (or pattern of transactions):

1. involves funds that come from illegal activity or are part of a transaction designed to conceal the funds are from illegal activity;
2. is designed, such as through structuring, to evade the reporting thresholds of the Bank Secrecy Act (BSA);
3. does not appear to serve any business or apparent lawful purpose and/or
4. uses either the FCM or IB to facilitate a criminal transaction.

FCMs and IBs should keep in mind the definition of transaction is very broad and is not limited to transactions conducted on a designated contract market or a derivatives execution transaction facility.

The SARs rule also permits firms to file reports for suspicious activity that is not required to be reported by the rule (e.g. a transaction below the $5,000 threshold).

As per government regulations, the suspicious activity report (SAR) must be filed with FinCEN at a central location that is noted on the filing instructions within thirty days after the FCM/IB becomes aware of a suspicious transaction.

However, if the FCM/IB is not able to identify a suspect, the filing date may be extended an additional thirty days in order to attempt to identify the suspect. The report must be made on Form 101 SAR-SF, which is the same form used by broker-dealers.

The federal government regulations state that where more than one FCM and/or IB is involved, only one form needs to be filed, provided the report contains all the relevant facts.

FCMs and IBs may consult and share information (including the SAR-SF) with each other in order to file a single report. A copy of the form and any supporting documentation must be maintained by the filing firm for a period of five years from the date of the filing.

Other firms involved in the transaction, but not filing the report, should also maintain a copy of the report.

FCMs and IBs may share an SAR, or any information that might reveal the existence of an SAR, with an affiliate, provided that affiliate is subject to an SAR regulation issued by FinCEN or another regulatory agency. However, the affiliate may not share the existence of the SAR, or any information that would reveal the existence of the SAR with another affiliate, even if that affiliate is subject to an SAR rule. In addition, the FCM or IB, as part of its internal controls, must have policies and procedures in place, which ensure its affiliates, protect the confidentiality of the SAR.

Exceptions to filing an SAR

1. FCMs and IBs are not required to file form SAR-SF for activity related to a robbery or burglary, provided the activity is reported to the appropriate law enforcement agency.
2. FCMs and IBs are not required to file an SAR for a violation of the Commodity Exchange Act, CFTC regulations, Exchange or NFA rules committed by the FCM or IB or any of their officers, directors, employees or Associated Persons provided this activity is properly reported to the appropriate agency. However, if this activity also involved a violation of the Bank Secrecy Act, FCMs and IBs must file the form SAR-SF.

Confidentiality

FCMs and IBs and their officers, directors, employees and agents are prohibited from disclosing (except to appropriate law enforcement or regulatory entities) that a transaction has been reported. This applies not only to the SAR, but also to any information that would reveal the existence o an SAR. This disclosure prohibition applies to all persons except as specifically authorized by the regulation.

FCMs and IBs are not prohibited from sharing or disclosing the existence of a SAR to appropriate law enforcement agencies or regulatory agencies, including the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the SEC, the CFTC, NFA and other self-regulatory organizations of which they are members, as provided by the suspicious activity reporting rules. In addition, when requested by one of these agencies, FCMs and IBs are required to provide these agencies with any supporting documentation to an SAR.

Risk based measures to help ensure the confidentiality of SARs include establishing restricted areas for reviewing SARs, maintaining a log of access to SARs, using cover sheets for SARs and supporting documentation that indicates the filing of an SAR and using electronic notices that highlight confidentiality concerns before a person may access or disseminate the information.

The existence of an SAR must not be disclosed, even under the guidance herein, if the securities broker-dealer, mutual fund, futures commission merchant or Introducing Broker in commodities has reason to believe it may be disclosed to any person involved in the suspicious activity that is the subject of the SAR.

Safe Harbor

The SARs rules also provide FCMs, IBs and their officers and directors, employees and agents with a statutory safe harbor against private civil claims brought by customers or others for any disclosures contained in form SAR-SF or for failure to disclose that a report has been filed, providing the regulatory requirements are met. This safe harbor applies equally to filings that are made on a voluntary basis.

SARs Summary

A Suspicious Activity Report has often been the springboard to enable law enforcement to find, arrest and convict money launderers. Your obligation to be 'tuned in' to suspicious activity is critical to this effort.

Alerting the authorities is not a casual responsibility. In a speech before Congress, Mr. Robert Werner, then Chief of Staff of the Treasury's Financial Crimes Enforcement Network said, "…of the 1,347 calls to FinCEN's hotline to date, 857 were of sufficient merit to be turned over to law enforcement."

Don't think your concerns or suspicions are necessarily unfounded! If you're not sure, err on the side of caution. It's better to report suspicious activity to your Director of Compliance that ultimately does not require an SAR than ignore any suspicious activity that does.

Red Flags — SARs

Red Flag checklists are a critical part in the process of monitoring for and detecting suspicious activity.

It is important to use Red Flags to monitor for suspicious activity after the account is opened. However, you must also be vigilant for suspicious activity as the account is opened or attempting to be opened. Section Three of this course contains CIP Red Flags to check, as you look for suspicious activity when opening an account.

If you opened an account that was initially 'red flagged', you may need to be particularly watchful monitoring that account for suspicious activity, paying particular attention to trading and movement of funds in and out of the account.

Here is a list of SAR Red Flags to help you monitor for suspicious activity from the Commodity Futures Trading Commission, Financial Crimes Enforcement Network, National Association of Securities Dealers, National Futures Association, Securities Industry Association and various FCM and IB compliance officers.

1. A customer account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
2. A customer requests cash disbursements.
3. A customer's account shows numerous cashier's check transactions aggregating to significant sums.
4. A customer's account has a large number of wire transfers to or from third parties who have no family or fiduciary relationship.
5. A customer's account has wire transfers at off times or to or from unusual locations, such as to or from a bank secrecy haven or country identified as a money laundering risk.
6. Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds or other assets.
7. The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.
8. A customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions to your policies relating to the deposit of cash or cash equivalents.
9. A customer engages in transactions involving cash over $10,000 or cash equivalents or other money instruments that appear to be structured to avoid government reporting requirements, especially if the monetary instruments are in an amount just below reporting or recording thresholds and/or are sequentially numbered.
10. A customer deposits funds to purchase a long-term investment, followed shortly thereafter by a request to liquidate the position and transfer the balance out of the account.
11. A customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
12. A customer requests that a transaction be processed in such a manner, to avoid your company's normal documentation requirements.
13. A customer deposits bearer bonds followed by an immediate request for the disbursement of funds.
14. A customer's account indicates large or frequent wire transfers immediately withdrawn by check.
15. A customer's account shows a high level of account activity with very low levels of futures transactions.
16. A customer exhibits an unusual level of concern for secrecy, particularly in regard to the customer's identity, type of business or sources of assets.
17. A corporate customer lacks general knowledge of his/her own industry.
18. A customer appears to be acting as an agent for another entity or individual but is evasive about the identity of the other entity (except a situation involving the identity or ownership interests in a collective investment vehicle).
19. A customer is from, or has accounts in, a country identified as a haven for bank secrecy, money laundering or narcotics production.
20. A customer who was not solicited or became a customer through the 'broker of the day'.
21. Trading with little or no risk.
22. Transactions and/or volumes of aggregate activity inconsistent with the expected purpose of the account and expected levels and types of account activity stated by the account holder at the time of the account opening.

If you know of any SAR Red Flags that are not on this list, we would appreciate it if you would tell us about them. We'd like to include those that are appropriate in our next periodic update of this course. Please email any suggestions to: WalshAMLEthics@gmail.com. Please write SAR Red Flag in the subject line of the email.

If you have any concerns, worries, questions or ambivalence as you monitor your accounts and encounter possible suspicious activity, **don't ignore them!** Talk with your IB's Compliance Officer or talk with the appropriate personnel in your FCM's Compliance Department.

AML Audits

The National Futures Association's AML Compliance Rule 2-9 (c) reports the government's AML rules to NFA members. This rule explains how the federal regulations require FCM and IB members provide for annual independent testing of the adequacy of their money laundering compliance programs.

An FCM or IB can satisfy this requirement with its own personnel that are independent of the personnel working in the areas exposed to potential money laundering or by hiring an outside party with experience in this type of auditing.

In either circumstance, the audit function should test all affected areas to ensure that personnel understand and are complying with the AML policies and procedures and that these policies and procedures are adequate. The results of any audit should be documented and reported to the firm's senior management or an internal audit committee or department and follow up should be done to ensure any deficiencies in the firm's AML program are addressed and corrected.

Investment Reference, an independent contractor, conducts annual audits of IBs, including AML audits. They report you don't have to be worried if your AML policies and procedures are to be audited, providing you are complying with all the regulators' AML rules and regulations.

I. Objective and scope of an AML audit

The audit is conducted pursuant to the National Futures Association's compliance rule 2-9 (c). The objectives of the audit are to determine if the IB being audited has, and is adhering to, anti-money laundering regulations as prescribed under the programs of said IB and its Futures Commission Merchant.

Additionally, if any corrective actions are required, they will be discussed with the management of the IB, and new issues regarding the IB's Anti-Money Laundering Program (AMLP) will also be discussed. If it is found that any corrective measures need to be taken, they will be detailed in this report and the signature of the principal of the subject IB on the audit form indicates that he or she is aware of those required actions and will take corrective measures.

The audit includes: a review of the current requirements under the AML program of the IB and its FCM, a discussion with the principals and Associated Persons of the IB to ensure they know what is required of them under the Anti-Money Laundering Program (AMLP), the CIP and SAR 'red flags' and the consequences of not complying with AML rules and regulations.

The name of the Compliance Officer is included in the final report. The required on-going employee training program is discussed. During the audit, it is suggested the principal(s) and APs re-read the AMLP to ensure they know it well.

There is a review of any accounts that have been submitted to the IB's FCM because of suspected suspicious activity and the results of any such submissions. If any such reports have taken place, verification is conducted with the FCM that the FCM has received the reports from the IB. A review of customer account files is performed to ensure any items required under the AMLP are being obtained and maintained in the customer's file. Deficiencies will be included in the audit report.

II. Recommendations for improving AML Programs

Any recommendations for improving the internal procedures for the audited IB, and/or adherence to those procedures will be conveyed to the principal(s) of the IB and included in the AMLP section of the audit report. Any recommendations for improving the IB's AMLP will be conveyed to the compliance officer, in writing.

III. Discussion of any noted deficiencies and an action plan to correct

Deficiencies (if any) are discussed with the principal(s). Deficiencies are included in the report. The 'comment' section notes suggest a plan for correcting deficiencies. Comments and suggestions are conveyed to the FCM in writing.

IV. Evaluation and opinion of the adequacy of the AML program

The overall evaluation and opinion of the adequacy of the AMLP will be stated in each audit report. If the program is believed to be inadequate, these notations will also be included in the 'deficiencies' section of the report, and the believed inadequacy will be brought to the attention of the compliance officer of the IB's FCM, in writing.

V. Senior management must sign a statement the audit was completed

Sample statement: "I affirm that on (date) an audit of our AMLP was completed by (name of auditor). I have been informed of the deficiencies found, if any, and the measures we must take to correct them. I further understand the deficiencies, if any, will be reported to our FCM."

A Member firm's written AML program should answer all of the following questions as completely as possible. Although you may answer "not applicable" to particular questions, you should carefully consider the firm's operations before doing so.

General Questions

- What is the firm's policy statement regarding money laundering and terrorist financing?
- What are the consequences if an employee does not follow the firm's AML policy?
- Who in senior management is responsible for giving written approval of the firm's AML program?
- Has the firm designated one or more individuals to be responsible for overseeing the day-to-day operations of the firm's AML compliance program?
- Whom has the firm designated?
- Does the AML Compliance officer/department report to senior management? If so, to whom do they report?
- What are the AML Compliance Officer's duties and responsibilities?

Customer Identification Program (CIP)

- What identifying information (e.g., name, address, date of birth, tax identification number) does the firm obtain from its new customers?
- Does the firm rely on documentary methods to verify identity? If so, what documents does the firm accept to verify the identity of new customers who are individuals? Be specific.
- What documents does the firm accept to verify the identity of new customers that are not individuals (e.g., corporations, partnerships, trusts)? Be specific.
- Does the firm rely on non-documentary methods to verify identity? If so, what non-documentary methods do the firm use to verify a customer's identity? Be specific.
- Under what circumstances will the firm verify identity:
- Using documentary methods alone?
- Using non-documentary methods alone?
- Using a combination of both methods?
- Does the firm require non-documentary methods in the following situations:
  - The customer is unable to present a current government ID with a photograph or similar safeguard (e.g., a thumbprint)?
  - The firm is not familiar with the documents the customer provides?
  - The firm opens an account without obtaining documents from the customer?

    - A customer opens an account without appearing in person?
    - Other circumstances that increase the risk that the firm will be unable to verify the identity of the customer through documents?
- If the firm does not use non-documentary methods in one or more of these situations, why has the firm concluded that non-documentary methods are not necessary?
- What is the firm's deadline for completing the verification process? How does the firm ensure that the customer's identity is verified within a reasonable time before or after the account is opened?
- Does the firm accept individual accounts from people who are applying for taxpayer identification numbers? If so, how does the firm confirm that an application for taxpayer identification number has been filed? How does the firm ensure that it obtains the taxpayer identification number within a reasonable period of time?
- Under what circumstances will the firm require customers that are not individuals (e.g., corporations, partnerships, trusts) to provide information about the account controller in order to verify the customer's identity?
- How does the firm handle an account if the firm does not have a reasonable belief that it knows the customer's identity? Specifically:
    - When will the firm refuse to open an account?
    - What restrictions do the firm place on customer transactions while the firm is still verifying the customer's identity?
    - Under what circumstances will the firm close an account after the firm's attempts to verify the customer's identity have failed?
    - In what situations will the firm file a suspicious activity report?
- Does the firm rely on other financial institutions to carry out its CIP requirements? If so, answer the following questions for each financial institution the firm intends to rely upon:
    - What is the financial institution's name?
    - When will your firm rely on that financial institution to perform some or all elements of the CIP for your firm? If it will perform only some elements, which ones are they?
    - What steps did your firm take to ensure that the financial institution is required to have an AML Compliance program under the Bank Secrecy Act?
    - What Federal agency regulates the financial institution?
    - When did your firm enter into a written agreement with the financial institution requiring it to certify annually that it has implemented an AML program and that it will perform the specified requirements of its own CIP or perform the CIP functions described in the agreement? (You should attach the agreement to the firm's AML procedures.)
    - How does your firm ensure that it obtains a copy of the annual certification?
- Does the firm contractually delegate its CIP functions to other entities? If so, answer the following questions for each entity (including any financial institution not included above) that the firm intends to contractually delegate those functions to:
    - What is the entity's name?
    - What elements of the firm's CIP are delegated to that entity?
    - When did you enter into a written agreement outlining each party's responsibilities? (You should attach the agreement to the firm's AML procedures.)
    - What does your firm do to monitor how the other entity implements the CIP and how effective the CIP is?
    - How does your firm ensure that regulators are able to obtain information and records relating to the CIP performed by that entity?
- How does your firm notify customers about why the firm requests information to verify identity before opening an account? What does the notice say?
- Where, in what form, and for what time period does the firm keep the following information:
    - Identifying information collected from customers (e.g., name, address, date of birth, tax identification number)?
    - Documents used to verify identity? Does the firm keep a copy of the documents or does it record the necessary information (e.g., identification number, place issued, date issued, expiration date)?
    - Descriptions of the methods used and results obtained when non-documentary methods are used to verify identity?
    - Descriptions of how discrepancies in particular customers' verifying information are resolved?

Identifying High-Risk Accounts

- How does the firm identify potentially high-risk accounts?
- What type of accounts does the firm characterize as high risk?
- How does the firm determine whether a customer/prospective customer appears on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN Report) identifying known or suspected terrorists and terrorist organizations?
- How does the firm determine whether a customer is located in a country on OFAC's list of sanctioned countries?
- How does the firm determine whether a customer appears on any list of known or suspected terrorists or terrorist organizations that is issued by the Federal Government and designated by the Treasury Department? How does the firm ensure that it follows all Federal directives issued in connection with the list? (Note: No other lists or federal directives have yet been issued).
- How does the firm determine whether a customer is from a country that appears on FATF's list of uncooperative countries (NCCT list)?
- What kind of due diligence does the firm perform to determine whether to accept a high risk account?
- How does the firm determine whether additional monitoring of account activity is necessary for a high risk account?
- What additional monitoring does the firm perform for account activity in high risk accounts?
- What special steps will the firm take if the customer/prospective customer or its country appears on the following lists:
    - OFAC's SDN Report?
    - OFAC's list of sanctioned countries?
    - A list of known or suspected terrorists or terrorist organizations issued by the Federal Government?
    - FATF's NCCT list?

Suspicious Activity

- What systems and procedures do the firm use to detect and report suspicious activity:
    - During the account opening process?
    - While an account is open?
    - When an account closes?
- What type of transactions will require the firm to file a form SAR-SF?
- How does the firm monitor wire transfer activity for unusual transfers (e.g., unexpected or unusually frequent or large transfers by a particular account during a particular period, transfers involving certain countries identified as high risk or uncooperative)?
- What examples of "red flags" does the firm provide its employees to alert them to suspicious activity?
- What kind of investigation does the firm do when a red flag occurs? Who does it?
- How promptly must employees report potential suspicious activity and to whom do they report it?
- Which supervisory personnel evaluate the activity and determine whether the firm is required to file a Suspicious Activity Report (i.e., SAR-SF) with FinCEN?

Other

- If your firm is an FCM, what steps does the firm take to respond to FinCEN information requests (e.g., 314(a) biweekly request)?
- If responsibilities for conducting AML compliance, other than CIP responsibilities, are divided between your firm and an FCM or IB, what documentation does your firm maintain to indicate how those responsibilities are divided? How does the firm ensure the other firm is adhering to the AML procedures?
- If your firm is an FCM that guarantees introducing brokers ("GIB"), how does it ensure that the firm's GIBs are adhering to their AML procedures?
- If your firm is an FCM, how does your firm comply with the currency transaction reporting and funds transfer record keeping requirements set forth in the Bank Secrecy Act?
- Does your firm accept private banking accounts maintained for non-U.S. persons? If so, what kind of special due diligence does the firm perform for those accounts? If not, how does the firm screen new accounts to ensure that it does not accept this type of account?
- Does your firm accept private banking accounts maintained by or on behalf of senior political figures? If so, what enhanced scrutiny does the firm conduct for private banking accounts maintained by or on behalf of senior political figures? If not, how does the firm screen new accounts to ensure that it does not accept this type of account?
- Which individuals or departments are trained, at least annually, on the firm's overall AML program?
- Which individuals or departments are trained to monitor unusual trading activity to detect suspicious activity? How often do these employees take the training?
- Who conducts the training and what areas does it cover? Be specific for each group of employees who receive training.
- Other than documents obtained or made during the CIP process, what AML documents and records does the firm maintain? How long are they maintained? Be specific.
- Which independent firm personnel or experienced outside party will conduct annual testing on the adequacy of the firm's anti-money laundering program?
- What areas are reviewed in the annual audit?
- Who in senior management or on the audit committee receives the results of the independent audit?
- How will the firm address deficiencies noted in the annual AML audit report?

Congratulations

Congratulations, you have completed this AML Compliance Training.

Be sure to read, understand and comply with your firm's AML Policies, Procedures and Controls.

Click the Sworn Declaration link below and fill out the form. When we receive it, we'll register and record your certification and send you a copy of your AML Certificate within three business days.

Your certificate **(not your Sworn Declaration)** is your proof you have successfully completed this course. **Please print carefully. We want your certificate to have the correct spelling of your name and other data for our records.**

Walsh Agency Inc. maintains all required records including: trainer's name and qualifications, course content, a detailed outline of all required subjects covered, persons certified, their date of birth, date course completed, a signed attestation the registrant read the required AML material and will comply with the rules and regulations, copies of Sworn Declarations and all other training materials for a minimum of the required five years from when the records were made.

Continue to Sworn Declaration

Contact Us

Walsh Agency, Inc
Telephone: (410)-207-0134
Email: rcounts@walshagencyinc.com
Address: 3019 Pebble Beach Drive
Ellicott City, MD 20142