AML: a Primer for Broker-Dealers

By Laura H. Goldzung

On October 26, 2001, President George W. Bush signed into law the USA PATRIOT Act. Title III of the PATRIOT Act imposed obligations on broker/dealers under new anti-money laundering (AML) provisions and amendments to the Bank Secrecy Act (BSA) in an effort to make it easier to prevent, detect, and prosecute money laundering and the financing of terrorism. Broker/dealers were required to have an AML compliance program in place as of April 24, 2002, and NASD Rule 3011, now FINRA Rule 3310, prescribed that each member develop and implement a written risk-based AML program *reasonably designed* to achieve and monitor compliance with the requirements of the BSA and its implementing regulations.

The purpose of this article is to discuss the history and the evolution of the requirements for an AML program here in the U.S., and to provide some context around these regulations to provide a better understanding of how operating here in the U.S. fits with global AML efforts.

The international standards setters:

- United Nations, the first international organization to undertake significant action to fight money laundering on a truly worldwide basis
- Financial Action Task Force (FATF) – formed by the G7 countries, promotes the adoption of international AML/Combatting Financing of Terrorism (CFT) standards for all countries: "FATF 40+9 Recommendations"
- Basel Committee on Banking Supervision – formed by the central bank governors of the Group of 10 countries
- International Association of Insurance Supervisors (IAIS) – insurance supervisors from more than 100 different countries and jurisdictions
- International Organization of Securities Commissioners (IOSCO) – regulatory bodies from 105 countries
- Egmont Group of Financial Intelligence Units - comprised of 94 jurisdictions

Laura H. Goldzung is President and Principal Examiner of AML Audit Services, LLC, an anti-money laundering and fraud consultancy specializing in independent testing and compliance consulting services to financial and nonbank financial institutions.*

The regional bodies and relevant groups:

- FATF-Style Regional Bodies (FSRBs) – are to their regions what FATF is to the world – promotion and implementation of AML and CFT standards within their respective regions
- Wolfsberg Group – established sets of principles for Private Banking
- Commonwealth Secretariat – voluntary association of 54 countries that support each other and work together towards shared goals
- Organization of American States (OAS) – regional body for security and diplomacy in the Western Hemisphere
- CICAD – Inter-American Drug Abuse Control Commission to confront the growing problem of drug-trafficking

The history of U.S. money laundering legislation:

- 1970 Bank Secrecy Act
- 1986 Money Laundering Control Act
- 1990 Financial Crimes Enforcement Network (FinCEN)
- 1992 Annunzio-Wylie AML Act
- 1994 Money Laundering Suppression Act
- 1996 Mandatory Suspicious Activity Reports (Banks)
- 1998 Money Laundering and Financial Crimes Strategy Act
- 2001 USA PATRIOT Act; Title III International Money Laundering Abatement & Anti-Terrorist Financing Act of 2001
- 2004 Intelligence Reform & Terrorism Prevention Act of 2004
- 2006 Regulation K Enacted (Edge Agreement Requirements for US Representative Offices)

The Bank Secrecy Act

The Bank Secrecy Act requires financial institutions to assist in the detection and prevention of money laundering and, specifically, requires financial institutions to keep records of cash purchases of negotiable instruments and file reports of more than $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion or other criminal activities. The BSA provides regulations for financial institutions defined as:

- Banks, thrift institutions, securities dealers, investment companies, insurance companies, dealers in precious metals, stones or jewels, pawn brokers, residential mortgage loan originators (RMLOs);
- Loan and finance companies, travel agencies, telegraph companies, credit card companies, automobile, boat and airplane dealers, real estate and settlement agents, casinos;
- Money services businesses including currency dealers or exchangers, check cashers, issuers and sellers of traveler's checks, money orders, prepaid access, money transmitters and any other person engaged as a business in the transfer of funds.

BSA reporting & recordkeeping requirements include:

- **Currency Transaction Report** (CTR) is required for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency of more than $10,000**.** Record retention is 5 years.
  - Designation of [CTR] Exempt Person – Exempt customers are designated in accordance with the requirements; the financial institution reviews and verifies information concerning exemptions at least and biennial filings are performed on required accounts; the financial institution adequately monitors exempt persons for suspicious activity; and exemptions are revoked when they no longer meet the regulatory criteria.
- **International Transportation of Currency or Monetary Instruments Report** (CMIR) is required for those who physically transport, mail or ship, or cause to be physically transported, mailed, shipped or received, currency, traveler's checks, and certain other monetary instruments in an aggregate amount exceeding $10,000 into or out of the United States. Record retention is 5 years. You may recognize this declaration on the customs form when flying internationally.
- **Foreign Bank Account Report** (FBAR) is required to be filed when the broker-dealer has an interest in or signatory or other authority over one or more bank, securities, or other financial accounts in a foreign country if the aggregate value of such accounts at any point in a

calendar year exceeds $10,000. The form and the account information are retained for 5 years.

- **Suspicious Activity Report** (SAR) is filed for any transaction conducted or attempted to be conducted through a broker-dealer that involves at least $5,000 in funds or other assets and that the broker dealer knows, suspects or has reason to suspect is relevant to a possible violation of law or regulation. Record retention from date of filing is 5 years.

Additional BSA record keeping requirements include:

- Funds Transfers Recordkeeping and Travel Rule: Collect and retain identifying information for the origination/ receiving information in connection with funds transfers of $3,000 or more. Retention is 5 years.
- Customer Identification Program (CIP): Identifying information must be retained for five years after the account is closed, including:
  - records related to the documents relied upon to verify customers' identities plus descriptions of the methods used and descriptions of the resolution of any substantive discrepancy discovered when verifying identifying information for five years after the record is made
- Monetary Instrument Sales Records (Bank Checks/Drafts, Cashier's Checks, Money Orders & Traveler's Checks) for $3,000 or more in currency, must obtain certain information and verify the identification of the purchaser. Record retention of the information is 5 years.

Chart 1. The Civil & Criminal Penalties for Money Laundering & BSA Violations

Money Laundering	▪ 20 years in prison ▪ $500,000 fine ▪ Forfeiture of property including bank accounts
Willful violation of the BSA by an employee of FI	▪ 5 years in prison ▪ $250,000 fine
FI violating certain provisions of BSA	$1M or twice the value of the transaction

U.S. Federal Statutes that Criminalize Money Laundering – Title 18 US Code

- Criminal prosecution of money laundering is a significant focus of US Government as well as international governments
- The tools and techniques developed to detect and prosecute the laundering of the proceeds of drug trafficking and financial crimes have been adapted for the war on terrorist financing, and include the above referenced Bank Secrecy Act reports

Title 18, US Code, Section 1956(a)(1)

Four Elements of the Crime:

- Conduct, or attempt to conduct, a financial transaction
- With the proceeds of a "Specified Unlawful Activity"
- Knowing, suspecting or being "Willfully Blind" to the fact that funds were from unlawful activity

With an objective to:

- Promote a specified unlawful activity
- Evade US taxes
- Conceal or disguise the source ownership / nature of the funds
- Avoid Federal or State transaction reporting requirements

Penalties: Up to 20 Years Incarceration and/or fine of the larger of twice amount of funds involved or $500,000.

The USA PATRIOT Act

The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Re-quired to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." While all broker-dealers must comply with the PATRIOT Act and the implementing regulations in 31 C.F.R. Part 1023 ("AML Rules"), the application of the rules may vary from firm to firm. For example, the application of certain AML rules may differ depending on whether a firm is retail or institutional, and whether a firm is an introducing or clearing broker.

The USA PATRIOT Act amended the Bank Secrecy Act multiple times and included:

- Enhanced due diligence for correspondent and private banking accounts

- Allows financial institutions to share information about customers
- Requires issuance of regulations establishing minimum standards to be followed by financial institutions in identifying new customers

Chart 2. Key Provisions of the Act:

Section 311	Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern
Section 312	Special Due Diligence for Correspondent Accounts and Private Banking Accounts
Section 313	Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks
Section 314	Cooperative Efforts to Deter Money Laundering (Information Sharing)
Section 319	Forfeiture of Funds in U.S. Interbank Accounts & Availability of Records
Section 326	Customer Identification Program (CIP)
Section 352	Anti-Money Laundering Program

Information Sharing with Law Enforcement

In response to requests from FinCEN under Section 314(a) of the PATRIOT Act, broker-dealers are required to have policies and procedures in place to respond to requests to conduct searches for transactions or accounts whether current or maintained during the preceding 12 months. A designated person must be identified to protect the security and confidentiality of the requests, and to ensure responses are made timely should an account or transaction be identified. Broker-dealers' process should include documenting evidence of the searches.

Voluntary information sharing under Section 314(b) allows firms to share information with other financial institutions by submitting an annual notice to FinCEN each year. Policies and procedures must be in place to process information shared among institutions, including procedures to safeguard the security and confidentiality of such information. The firm must verify that the financial institution it intends to share information with has filed notice with FinCEN; this information is available at FinCEN's website. Firms should retain the FinCEN acknowledgement in a secure and confidential file. You can expect a review of the acknowledgement during your annual AML audit.

FINRA

Broker-Dealers & FINRA Rule 3310

Section 352 of the PATRIOT Act requires broker-dealers to establish a written AML program that is *reasonably designed* to achieve and monitor compliance with the requirements of the BSA and its implementing regulations. Under FINRA Rule 3310, the AML program must be approved, *in writing*, by the firm's senior management and must include:

- Procedures to detect and cause reporting of suspicious activity
- Procedures to achieve compliance with the Bank Secrecy Act
- Designation of an AML compliance officer
- Ongoing training
- Independent testing

Two key phrases are used in the AML world: reasonably designed and risk-based. Broker-dealers are expected to have a reasonably designed, risk-based AML program tailored to the business of the firm. And while it is not a requirement to have a risk assessment, it is both a regulatory expectation and a best practice. The AML program should be commensurate with the risk profile, which only makes sense if indeed it is risk-based.

Role of Regulators & Their Expectations

Regulators are responsible for ensuring that financial institutions comply with the BSA and follow requirements to combat money laundering and terrorist financing. Regulators examine compliance programs for adherence to regulations, may impose civil fines and refer matters for criminal prosecution, and issue cease and desist orders, fines, and censures for non-compliance.

The Three Stages of Money Laundering

A review of the three stages of money laundering helps to distinguish where broker-dealers have risk; generally, it is in the layering stage. The integration phase of money laundering can be more difficult to detect than placement.

Money Laundering Typologies

Proceeds of crimes can be associated with more than drug trafficking. Crimes can be associated with the following typologies:

- Financial fraud
- Computer crimes

- Human smuggling
- Illegal arms sales
- Illegal gambling
- Corruption of foreign officials
- Terrorist financing

Terrorist Financing

Terrorist Financing supports the agenda, activities or cause of a terrorist organization. Funds raised may come from legitimate sources, such as charitable organizations or donations, and can also come from criminal sources and illegal activities, such as drug trade, weapons smuggling, fraud, kidnapping and extortion.

- Can involve legally derived funds
- Disguise association between themselves and funding sources
- Generally smaller sums

The Four Pillars

AML compliance programs contain the known "Four Pillars" of compliance that apply to all financial institutions under the BSA:

- Policies, procedures and internal controls;
- Designation of an AML compliance officer;
- Ongoing training for appropriate personnel; and
- Independent review.

So let's address each of these "pillars" and explore the various requirements within.

Pillar One: Policies, Procedures & Internal Controls

Policies, procedures and internal controls are the heart and soul of an AML compliance program. Establishing policies sets into motion the statements that will drive procedures and the internal controls associated with them. You can view this as the why and the how.

Typically this begins with the firm's AML policy which establishes the over-arching theme for the AML compliance program, one that states the firm prohibits and actively prevents money laundering and any activity that facilitates money laundering or funding of terrorist activities by complying with all the applicable requirements under the BSA and its implementing regulations. This is followed by the definitions of money laundering and terrorist financing. Often, the firm will conclude this statement with a commitment to review and update the program as regulations, best practices and changes in the activities of the firm evolve.

Internal controls will describe various implementations around managing risk, starting with the risk assessment, and addressing all areas where policies meet processes. FINRA has an expectation that your firm will have internal controls in place to identify when circumstances change in such a way as to trigger previously inapplicable AML requirements and to amend your AML policies and procedures to accurately reflect all AML requirements that are applicable to your firm.

Chart 3.

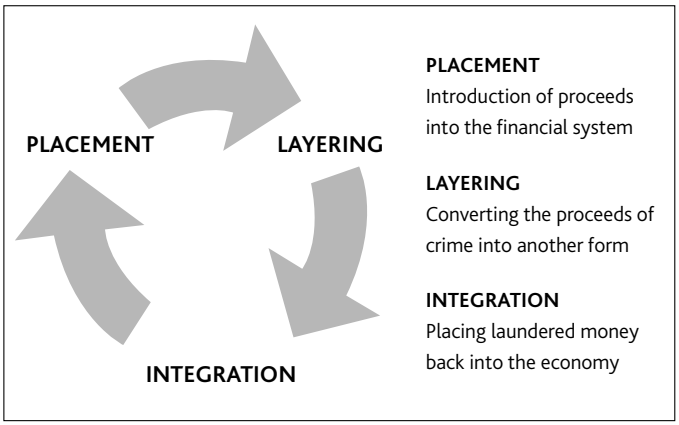

Chart 4. This graphic illustrates a Comprehensive BSA/AML Compliance Program

Source: Landon Associates

Pillar Two: Designation of the AML Compliance Officer

This policy identifies the person designated and the responsibilities for managing the day-to-day activities of the program. The AML Compliance officer is expected to have a working knowledge of the BSA and its implementing regulations and be qualified through knowledge, experience, and training. The activities of the compliance officer will include updating the program and the risk assessment, communicating with personnel and management about the program's adequacy, risks, and reporting activities, liaising with regulators and internal or external audit, coordinating AML training for appropriate personnel, managing transaction monitoring systems for detecting and monitoring suspicious activities, and reporting and record-keeping. While this is not an exhaustive list, you get the picture: it is a big job. Firms would be wise to ensure that the compliance officer can execute his or her duties with adequate authority and resources. Direct reporting lines are important as well. The compliance officer is an effective partner in managing the risk of the firm, and having access to the decision makers in management will be paramount to good communications and safeguarding risk. Gone are the days when you could simply appoint the operations manager or branch assistant as AML compliance officer without the requisite knowledge and experience. The risk is simply too great.

Broker/dealers were required to have an AML compliance program in place as of April 24, 2002, and [to] develop and implement a written risk-based AML program reasonably designed to achieve and monitor compliance with the requirements of the [Bank Secrecy Act].

Pillar Three: AML Training

Training for appropriate personnel is essential to managing compliance risk and, driven by job function, should be comprehensive and sustainable. Front line personnel are generally the first point of contact when interfacing with customers and, when properly trained, can recognize red flags and escalate unusual or suspicious activity as prescribed in the policies and procedures. Training is typically given within a certain number of days of hire, and refresher training is given at least annually or as dictated by risk, new product or service rollout, and other factors. Broker-dealers will leverage the required AML training by including the AML requirement as part of its Firm Element required training and the annual compliance meeting.

Training generally includes the regulatory reuirements and the firm's policies, procedures and processes. The program serves to reinforce the importance senior management places on the firm's AML compliance, ensuring that all employees understand their role in maintaining an effective AML compliance program. Training often consists of 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, how and to whom to escalate unusual activity, their role in the compliance efforts, reporting and confidentiality of Suspicious Activity Reports (SARs), disciplinary consequences for non-compliance with the BSA, and other topics appropriate to the job function of the personnel. Also described is the methodology used to train personnel, such as distribution of articles and regulatory updates, online or internet based modules, scenario-based training provided by a third party, seminars and in-person education programs, etc.

Firms who have historically limited AML training to the annual compliance meeting by including a few slides – take note that FINRA has an expectation that if you take your AML obligations seriously, you will provide effective and sustainable training. A couple of slides do not comprehensive make! A good rule of thumb, or best practice, is to provide a minimum of three training events. An example of this would be an update review of the policies and procedures; an online scenario-based module, and a seminar or in-person event.

Tracking and maintaining records is important and required. A good practice is to partner with your training department when conducting the training needs analysis and including the topic of AML. Enlist your training colleagues to develop engaging ways in which to include the topic. Work closely with lines of business to determine if new products or services will be rolling out. Be sure to have a seat at the table with marketing and training, to ensure that the AML compliance program is not at risk for failing to train in the AML aspects of new products or services.

Regardless of how you position it, AML training proves to be quite effective at alerting appropriate personnel to customers and transactions that may have money laundering risk. And you'll want to be sure that your firm has little exposure.

Pillar Four: Independent Testing

The fourth pillar calls for an independent audit function. Do not let the terminology confuse you – independent audit, test and review are interchangeable. Whether you are part of a larger firm with an internal audit department that is deemed to be independent, or you are in a mid-size or small firm that relies on third party subject matter consultants, the independent test establishes that your program meets the regulatory requirements. Unlike a financial audit, the independent AML audit judges the efficacy of the program and its satisfaction of regulatory expectations. Independent audit is an opportunity to identify if key controls are working, if the program is adequate, and if the overall design is effective for the firm.

How is independent defined? An AML audit may be conducted by firm personnel who are independent of any areas that are exposed to potential money laundering risks, or by a qualified outside party. Individual(s) performing the review must be independent of compliance management, any unit who performs a control(s) in the AML program, and compliance, internal audit, units performing AML control functions should not report to the same executive.

When internal audit is conducting the test, they already have a full understanding of the firm's products and services, customers, and the geographic areas that it serves. When an external resource is contracted, they must first come to learn the facets of the firm and the customers, products and the geographies that it serves. Often times, internal audit will co-source with an external resource. Why? AML/BSA may be only a small part of the internal audit's remit, and sometimes the internal audit personnel are not as up-to-date on the regulations and best practices as a subject matter expert (SME). SMEs are sometimes engaged to co-source with internal audit to assist in conducting the annual AML test, as subject matter experts are typically up to date on recent guidance, regulations, and best practices, and can serve to educate the internal audit personnel. The firms' AML audit committee typically makes the decision to co-source, and may engage every few years with a subject matter expert. It is a win-win when subject matter experts are engaged to co-source, as each group can learn from the other and bring more independence to the table.

Where's the risk for broker-dealers?

Customer risk presents itself with online accounts, customer types (Politically Exposed Person (PEP), non US-customer, hedge funds, charities), and entities that obscure ownership or beneficial interest (LLCs, Private Investment Company (PIC), offshore trusts). Geographic risk, fairly easy to determine, is based on the location of the broker-dealer, locations of its customers and transactions, and offshore funding sources. Business risk is associated with the products and services offered, source of funds, investment objectives (variable annuities, derivatives, penny stocks, money movements – whether retail or institutional), and intermediated accounts.

Risk Assessment

Broker-dealers have an obligation to identify, measure, monitor and control AML and Economic Sanctions Risk, and the risk assessment is the tool used to enable the firm to achieve this goal. It is the foundation, driver and a required component of a sound BSA/AML Program. With globalized capital markets, trading vulnerabilities due to securities fraud and market manipulation, and rapid money and asset movement, it stands to reason that conducting a comprehensive risk assessment will serve a firm well. There is no real standard format. However, the AML community looks to the *Federal Financial Institutions Examination Council* FFIEC exam manual as the gold standard for guidance. Each broker-dealer needs to determine appropriate format and level of complexity of the risk assessment to effectively identify, evaluate and measure BSA/AML risk. Certainly, a complex broker-dealer with multi-national business units will require a risk assessment to match, while the small firm's risk assessment will be of a lower complexity. While the Board of Directors is ulti-mately responsible for AML risk, many people will read the risk assessment, including the Board of Directors, executive management, chief compliance officer, general counsel, internal/external audit, and FINRA, SEC and State examiners.

There are 4 essential elements in a risk assessment:

- Executive Summary
- Methodology
- Assembly, i.e. template used
- Action Plan to resolve weak controls

Your ultimate goal is to prevent the firm's products and services from being used to facilitate money laundering and terrorist financing. More importantly, the risk assessment informs the AML policies and procedures. The risk assessment is an internal control designed to identify risks and provide for mitigants to manage the risk. It is a dynamic process that has a direct link to future activities, one which requires ongoing evaluation of the firm's risks and controls as new risks are identified.

The Bank Secrecy Act requires financial institutions to assist in the detection and prevention of money laundering….

Let's say, for example, you are the AML Compliance officer and your marketing department has just announced a new product launch. You were caught unaware because you did not have a seat at the table during discussion. Together with the business owner, you quickly formulate a risk assessment of that product or service and those clients who are likely to invest in those products. Your result may indicate a band-aid process is needed because you do not have the appropriate time before roll-out to put into place several efficient steps of mitigation. This results in a patchwork plan, with higher inherent risk than is optimal, and you now have to deploy resources you were expecting to use on another project.

A dynamic process, the risk assessment offers opportunities to strengthen controls and mitigate gaps on an ongoing basis. Just as the AML program is informed by the risk assessment, so too is the risk assessment informed by the AML program.

Connecting the Assessment to Detection

Connecting the periodic assessment to detection is where the rubber meets the road. By identifying existing Red Flag detection points, building a specialized suspicious activity detection program and a SAR investigation and reporting infrastructure, a firm will use the risk assessment to drive adequate suspicious activity monitoring.

Doesn't the Clearing Firm Have Responsibility?

The clearing firm is not responsible for monitoring your AML program, although they do employ transaction monitoring systems and often times will offer a set of AML-related exception reports to the firm. Do not mistake that for obligation. They have their own AML obligations and surely your independent auditor will ask for a copy of their annual AML Certification letter indicating their compliance with the regulations. If you have a reliance agreement whereby they provide dual controls with certain processes, or even take on responsibilities, your firm is still responsible on its own. The firm must ensure any third party, including the clearing firm, is adequately performing its agreed processes.

The firm is responsible for detecting, monitoring and reporting, as well as maintaining the records. The firm must determine if higher risk customers are worth the compliance cost and, more importantly, the risk, to maintain the account. The firm must determine what risk tolerance it is willing to absorb. One client running amok can impact regulatory and compliance risk, credit risk, and reputational risk, and no one wants to see the firm's name in the headlines. In the end, are the profit margins worth the risk? The risk assessment allows management to gauge its exposure and that is why conducting the risk assessment is a best practice.

A Breakdown of AML Policies

- Customer Identification Program (CIP)

The CIP outlines the required information set forth under the regulations, the methods employed to verify the information, dealing with customers who refuse to provide information, the lack of verification, reliance on another institution to conduct verification of identity, comparison with government-provided lists of terrorists, customer notification and record-keeping requirements. CIP is a minimum requirement which includes the basics: name, address, date of birth and taxpayer identification number. Customer verification must be risk-based and conclude within a reasonable time before or after the customer's account is opened, either by documentary or non-documentary means - or both. Verification for an individual is typically in the form of an unexpired government-issued identification evidencing nationality or residence and bearing a photo, such as a driver's license or passport. For entities, documents showing the existence of the entity such as certified articles of incorporation, business license, trust or partnership agreement. Non-documentary verification can be consumer

reporting agency reports, public or vendor databases, financial references or financial statements.

- Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD)

The CIP program is not to be confused with customer due diligence. CIP information alone does not allow the firm to form an opinion on the fitness of a customer to transact business. Rather, conducting customer due diligence (CDD) provides for sufficient information to understand the customer and the types of activities to be expected, the source of funds, customers' employment or business, and the like.

It enables the firm to predict with relative certainty the types of transactions in which the customer is likely to engage. When customers are deemed to be a higher risk or have transactions deemed questionable, the firm will conduct enhanced due diligence, documenting additional information the firm may use to monitor activities when informing its suspicious activity monitoring program. Another form of diligence known as Special Enhanced Due Diligence, or SEDD, is used with foreign bank customers, as seen in the banking sector. Here's how it all fits together:

Chart 5

CIP refers to information that must be obtained and verified at account opening to establish the true identit of a customer.	**CDD** refers to the basic information that is collected for all customers.
EDD refers to additional information that is collected for high risk customers.	**SEDD** refers to additional information collected for cusomers identified as foreign banks posing increased risks for ML.
KYC refers to all of the information obtained from CIP, CDD, EDD, and SEDD. KYC allows the institution to objectively gain an understanding of the customer's normal and expected activity and assists in indentifying unusual patterns or transaction anomalies.	

In the broker-dealer environment, there are a few rules that intersect around account opening. They are:

- Customer Identification Program (CIP) under Section 326
- SEC 17a-3(a)(17) provides regulators with access to books and records enabling BD's review for compliance with suitability rules.
- Customer Due Diligence
  - General Know Your Customer Requirements under FINRA Rule 2090
  - Specifically required due diligence, i.e., foreign correspondent accounts, private bank accounts

The AML program will also include the following policies:

- Correspondent Account for Foreign Shell Banks, including the detection and closing of correspondent accounts of foreign shell banks, certifications required, record-keeping for correspondent accounts of foreign banks, summons or subpoenas of foreign bank records and termination of correspondent relationships with a foreign bank.
- Due Diligence and Enhanced Due Diligence Requirements for correspondent accounts of foreign institutions including special procedures when due diligence or enhanced due diligence cannot be performed
- Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts or Senior Foreign Political Figures including methodologies and record-keeping.
- Special Measures for Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern as issued by FinCEN including procedures and process for reviewing account records and activities as prescribed.
- Clearing & Introducing Firm Relationships including the exchange of information, data and exception reports. Included would be if the firm has a reliance on the clearing firm to conduct any AML-related processes. While both entities have separate obligations to maintain an AML compliance program, the clearing relationship generally offers some features to complement the firm's anti-money laundering program.

Suspicious Activity Monitoring and Reporting

Seven Habits guru, Stephen Covey, is fond of saying "Begin with the end in mind," and one could say that a firm's suspicious activity monitoring program should be driven on this basis. We know that in the end customers and activities that are suspicious will indeed be reported using the Suspicious Activity Report (SAR), and those investigated and closed with or without a filing will both be fully documented and retained. It is all the steps that are taken when detecting activity – from initial alert all the way through escalation to the AML compliance department and ultimately the decision

whether to file the SAR that are so important. Having a system, no matter how simple or sophisticated, whether manual or automated, demonstrates appropriate diligence. Having a system of procedures and controls is important, in conjunction with a clear chain of escalation to supervisory or compliance department personnel. Simply identifying a red flag does not necessarily mean a report will be filed. Rather, it serves as a detection point or alert, requiring further diligence. No matter what, be sure to document your rationale, regardless of whether you file a SAR.

Office of Foreign Asset Control (OFAC)

While OFAC screening is not part of the BSA or PATRIOT Act regulations, many AML programs cover OFAC and the screening of customers against government and other relevant lists.

OFAC administers laws that impose economic sanctions against hostile foreign countries to further U.S. foreign policy and national security objectives. OFAC is also responsible for issuing regulations that restrict transactions by U.S. persons or entities (including banks) with certain foreign countries, their nationals, or "specially designated nationals." Violations of these laws can expose financial institutions to substantial penalties.

Large broker-dealers will develop and maintain OFAC policies, procedures and risk assessment, apart from the AML program. Other firms will simply include it in their policies and procedures manual. It is expected that firms will maintain an accurate, current listing of prohibited countries, entities, and individuals or have a Transaction Monitoring System (TMS) or third-party arrangement with a vendor or clearing firm to manage this process. Prior to opening an account, or conducting a transaction, the firm compares new accounts, funds transfers, or other transactions with the OFAC listings, and periodically compares established accounts and other customer transactions with the current OFAC listings. If your arrangement is for clearing or another party to manage this process for you, ensure that you know the frequency with which batch screenings are conducted for all customers of the firm, and who is responsible for blocking and rejecting transactions and report filings.

Recent Cases

We have seen a proliferation of money laundering and fraud cases in the media with some of the largest fines imposed – HSBC, Standard Chartered, Citi, to name a few. The size of the fines notwithstanding, it is safe to say that all of those financial institutions, in the end, had inadequate controls. Controls tie back to the adequacy and comprehensiveness of the risk assessment as does providing adequate training. The industry is made up of incredibly talented people who, when fully trained, can be a firm's first line of defense against financial crime. Strong ethics, good governance, skilled personnel, and a committed senior management team go a long way to combating financial crime. Keeping your AML program dynamic along with your perspective, and maintaining a sense of humor – all make for a good end. Begin with that!

ENDNOTES

* Laura H. Goldzung's additional expertise includes domestic and international training, design and development of BSA/AML compliance programs, risk assessment and analysis, remediation and corrective action programs, and expert witness consulting and testimony. She has worked with institutions that have been referred to enforcement for BSA/AML violations, helping them to bring their AML programs into compliance.

In her more than 25 year career in the financial services industry, Ms. Goldzung has worked in a variety of executive roles, most notably as Vice President and Managing Director at the Securities Industry Association (now SIFMA) and Executive Director of the Securities Industry Institute. During her tenure at SIA, she assisted member-firms in coordinating the implementation of the USA PATRIOT Act and the development of AML training. In prior years, she held a number of executive management and supervisory roles in the broker-dealer sector.

Ms. Goldzung is a Certified AML Specialist (CAMS) and Certified Fraud Examiner (CFE). She serves as an industry arbitrator for FINRA Dispute Resolution and is active with several industry groups including the Association of Certified AML Specialists, Association of Certified Fraud Examiners, National Society of Compliance Professionals, and SIFMA's Compliance & Legal and Internal Audit Societies, to name a few. She serves on a variety of industry task forces and committees, and serves as faculty for a number of industry education and certification programs. Ms. Goldzung is a frequent speaker and contributor on the topic of anti-money laundering and fraud.