ACAMS® NORTHERN NJ CHAPTER

ACAMS Study Guide Review

Thoughts

- Use the Index
- Outline
- Anonymous
- You’re seeking certification not expertise

Chapter 2

Risks and Methods of Money Laundering and Terrorist Financing

- FATF 40 – Financial Action Task Force
  - Paris based
  - 7 industrialized nations - intergovernmental
  - Foster international action against money laundering.

I. Three Stages of money Laundering

- Placement – Physical disposal of cash or other assets from criminal activity
  - Introduces criminal proceeds into financial system
- Layering – separating illicit proceeds from source by layers of financial transactions
  - Intent to conceal origin of proceeds
- Integration – Moving laundered funds into economy through normal business or personal transactions

II. The economic and social consequences of money laundering

- Increased Crime and Corruption – Crime becomes Attractive
- Undermining the legitimate private sector – no real profit
- Weakening financial institutions
  - Reputational risk – people don't want to do business with you.
  - Operational risk – loss resulting from inadequate internal processes
  - Legal risk – law suits
  - Concentration risk – to much credit to one borrower
- Economic Risk to a Country
  - Loss of control or mistakes in economic policy
  - Economic distortion
  - Loss of tax revenue
  - Risks to privatization efforts
  - Reputational risks to country
  - Social costs – makes crime profitable

III.a. Methods of Money Laundering

- Banks and Other Depository Institutions
  - Electronic Transfers of Funds
    - Xfer of funds from financial safe haven
    - Inconsistent with customer's business or history
    - Large incoming fund transfers received on behalf of a foreign client with no explanation
    - Many small incoming transfers which are immediately wired to a different city of country
    - Unexplained, repetitive or unusual activity
    - Payments or receipts with no link to legitimate contracts
    - Fund transfer sent or received to same person and different accounts
  - Correspondent Banking (bank to bank)
    - The provision of banking services by one bank(correspondent, to another, respondent)
    - Doing this internationally allows business worldwide.
    - Vulnerable because
      - Indirect relationships
      - Large volumes of transactions
      - Foreign countries have different AML requirements
      - No access to the quality of respondent bank's AML controls
      - Nesting – Correspondent bank offers services to other banks .

III.a. Methods of Money Laundering

Banks and Other Depository Institutions

- Correspondent Banking (cont.)
  - Patriot Act response to problems
    - » Sec 312 –
      - Risk based due diligence
        - Identify owners of foreign bank offshore or area of concern
        - Identify if foreign bank offers correspondent accts
        - Enhanced scrutiny of correspondent acct
    - » Sec 313
      - No correspondent accts with shell bank (no physical presence, not subject to inspection by a banking authority, no records)
    - » Sec 319
      - Keep records of names and contact information of owners of foreign banks who have correspondent accounts. Must also have name of US agent for service of process.

III.a. Methods of Money Laundering

Banks and Other Depository Institutions

- Payable-Through Accounts(A type of correspondent)
  - Customer directly control funds at correspondent bank.
  - May have unlimited amt of sub-acct holders.
    - PTA's with foreign institutions licensed offshore
    - Treat respondent bank as sole customer, no DD for PTA.
    - PTA subaccount holders can have deposit and withdrawal access
    - PTA in conjunction with subsidiary or rep from other office
- Concentration Accounts
  - Internal accounts used to process and settle multiple individual customer transactions usually same day. Many locations to one location -- -Customer data isn't always attached to transactions. Funds lumped together - danger
- Private Banking
  - Personalized banking for very rich people
  - Very competitive and profitable – included to do anything client wants

III.a. Methods of Money Laundering

Banks and Other Depository Institutions

- Structuring
  - Most common
  - Attempt to avoid reporting requirements
    - Cuckoo smurfing (switcharoo) people don't know they are part of a laundering scheme. Page 43. FATF recommends tracking depositors who pay into third party accounts.
    - Micro-Structuring – same as structuring only more smaller amounts.
- Bank Complicity
- Credit Unions or Building Societies
  - Although smaller than banks still a possible venue for money laundering

III.b. Methods of Money Laundering

- Non-Bank Financial Institutions
  - Credit Card Industry
    - More likely in the layering and integration stages
    - Not a cash focused industry so not usually part of placement
  - Money Remitters and Money Exchange Houses
    - Subject to a variety of national and local regulations
    - If banks work with money remitters must check for a license
  - Insurance Companies
    - Money Laundering vulnerabilities
      - due to investment aspects of life insurance policies – whole life or permanent life

III.b. Methods of Money Laundering

Non-Bank Financial Institutions

- Insurance Companies vulnerabilities (cont.)
  - Lack of oversight over intermediaries. Brokers have a lot of freedom.
  - Decentralized oversight over aspects of sales. Captive (employees) and non-captive agents.(independents)
  - Profit motive
  - Policies operate same as a mutual fund or trust. Customer overfunds and moves money around within policy, can be withdrawn.
  - Insurance bonds. Purchased and redeemed early.
  - Free-lock period/ early redemption
- Securities broker dealers
  - Vulnerable because
    - International
    - Speed of transactions

III.b. Methods of Money Laundering

Non-Bank Financial Institutions

- Securities broker dealers vulnerabilities (cont.)
  - Ease of conversion of holdings
  - Routine use of wire transfers
  - Profit driven business
  - Concealment of identities nominee accounts

III.c. Methods of Money Laundering

- Non-Financial Businesses and Professions
  - Casinos and Other Businesses Associated with Gambling
    - Usually placement stage(cash to checks)
  - Dealers in High-Value Items (Precious Metals, Jewelry, Art, etc.)
    - Patriot act required an AML program for these businesses
    - Gold very attractive – valuable, melted, small amt worth a lot.

III.c. Methods of Money Laundering

Non-Financial Businesses and Professions

- Dealers in High-Value Items (Precious Metals, Jewelry, Art, etc.) (cont.)
  - Payments or returns to persons other than owner
  - Precious metal pool accounts
- Travel Agencies
  - Purchase expensive airline tickets for other person and ask for a refund
  - Structuring wire transfers
- Vehicle Sellers
  - Structuring
  - Trade-ins buying and selling new
  - Third party payments

III.c. Methods of Money Laundering

Non-Financial Businesses and Professions

- Gatekeeper, Notaries, Accountants, Auditors and Lawyers
  - In the European Union and several other countries, mandatory anti-money laundering duties already apply to "gatekeepers." The FATF 40 Recommendations also cover independent legal professionals lawyers and legal professionals, and other "gatekeepers."
  - Why vulnerable
    - Create corporate vehicles/complex legal arrangements
    - Buying and selling property
    - Perform financial transactions
    - Provide financial and tax advice
    - Provide introductions to financial institutions
  - Identifying clients. Conduct DD.
  - Maintain records.
  - No tipping off client about investigation
  - Controversial as to lawyers in US. – Unless lawyers conduct international xactions

- Investment and Commodity Advisors
  - Withdrawal of assets to unrelated accts.
  - Frequent additions or withdrawals from accounts.
  - Third party with checks drawn on, or wire transfers
  - Clients request custodial arrangements/anonymous
  - Investing illegal proceeds for a client
  - Movement of funds to disguise origin

III.c. Methods of Money Laundering

Non-Financial Businesses and Professions

- Trust and Company Service Providers (what are they?)
  - Acting as a formation agent of legal persons
  - Acting as director or secretary of a company
  - Providing a registered office/business address
- Real Estate Industry
  - Buying or selling real estate to hide illicit sources of funds
  - Large number of diverse transactions.
  - “reverse flip” cooperative seller sells house below market price and accepts the difference under the table from ML person. ML person then sells house for market value.
  - “loan back” criminal gives associate illegitimate money. Associate then loans money back to criminal.

III.c. Methods of Money Laundering

Non-Financial Businesses and Professions

- Manipulation of Prices in Import and Export Transactions (trade based money laundering)
  - the process of disguising the proceeds of crime and moving value through the use of trade transaction
  - Over/under invoicing
  - Over/under pricing
- Black Market Peso exchange
  - a process by which money in the U.S. (could also be in another country, for example, countries in Europe) derived from illegal activity is purchased by Colombian (and other countries') "peso brokers" and deposited in U.S. bank accounts that the brokers have established. The brokers sell checks and wire transfers drawn on those accounts to legitimate businesses, which use them to purchase goods and services in the U.S.

IV. Money Laundering

Risks Associated with New Technologies

- Online or Internet Banking
  - Customer identification a large challenge
  - Huge cross border movements
  - Rapidity of ETF. Easy to make quick multiple complex transactions.
- Internet Casinos
  - Involves poorly regulated offshore accounts.
- Prepaid Cards and E-Cash
  - Anonymous card holders
  - Anonymous funding
  - Anonymous access to funds
  - High value limits or no limits
  - Global access to cash through atms
  - Offshore card issuers
  - Substitute for bulk cash smuggling

V. Money Laundering Risks of Structures Designed to Hide Beneficial Ownership

- Shell Companies
  - A company that at the time of incorporation has no significant assets or operations
    - Use of nominees as owners or directors
    - Layering
    - Loans
    - Fictitious business expenses/false invoicing
    - Sale of business
    - Buying a company already owned by the criminal enterprise
    - Paying out fictitious salaries
- Trusts
  - Assets placed under control of another person for the benefit of one or more persons. ANONOYMOUS
- Bearer Bonds and Securities
  - Can disguise legitimate owners.

VI. Terrorist Financing

- Differences and Similarities Between Terrorist Financing and Money Laundering
  - Money laundering – illegitimate funds/ legitimate use
  - Terrorist financing – illegitimate or legitimate funds/illegitimate use.
- Detecting Terrorist Financing – page 99
  - International wire transfers
  - Numerous attempts to withdraw debit atm in excess of limit
  - High percentage of withdrawals from debit cards
  - Low percentage of checks
  - Deposits and withdrawals immediately follow
  - Over all transactions below reporting requirements
  - Funding from cash and overseas wires
  - Series of transactions involving several hijackers at same atm.
  - Debit cards used by those with no accounts.

VI. Terrorist Financing

- Hawala and Other Informal Value Transfer Systems – page 105
  - "underground banking" are alternative remittance systems or informal value transfer systems
  - attractive for a launderer because it leaves little to no paper trail. The details of the customers who will receive the funds are faxed between the brokers.
  - used in any phase of money laundering

VI. Terrorist Financing

- Charities or Non-Profit Organizations
  - Enjoying the public trust.
  - Having access to considerable sources of funds.
  - Being cash-intensive.
  - Frequently having a global presence, often in or next to those areas that are exposed to terrorist activity.
  - Often being subject to little or no regulation and/or having few obstacles to their creation.
  - Money Laundering can be avoided if
    - Maintain a full program of budgets that account for all expenses
    - Conduct independent internal and external audits.

- 97 pages in 21 slides

  Don’t forget the review questions at the end of the chapter

Chapter 3

- FATF – **Membership**
  - Promulgating guidance for AML to governmental bodies.
  - IMF and World Bank both also offer important new perspectives in the field.
  - Criteria of membership
  - First step - evaluate
    - Size of GDP
    - Size of banking sector
    - Impact on global financial system
    - Regional prominence in AML/CFT efforts.
    - level of commitment to AML/CFT efforts.
    - Level of adherence to financial sector standards.
      - Participation in other relevant international organizations.
    - Level of AML/CFT risks faced and efforts to combat those risks.
  - Second Step - a written commitment to….
      - Endorsing and supporting the FATF 40 Recommendations,
      - Agreeing to implement all of the FATF Recommendations 3 years
      - Agreeing to undergo a mutual evaluation
      - Agreeing to participate actively in FATF
    - The country should be a full and active member of a relevant FATF-style regional body

FATF- Objectives

1. Spreading the anti-money laundering message worldwide
2. Monitoring implementation of the FATF recommendations among FATF members
   - An annual self-assessment exercise where member countries are required to fill out detailed standard questionnaires on the status of their compliance with the Recommendations
   - The more detailed mutual evaluation procedure. Each member country is examined by FATF
     - The experts write a report assessing the extent to which the evaluated country has moved forward in implementing an effective system to counter money laundering

FATF- Objectives (cont.)

- FATF does not have the power to impose fines or penalties against recalcitrant member-nations.
  - FATF launched a policy for dealing with nations that fail to comply with the FATF –'graduated approach'
  - The first step is requiring the country to deliver a progress report at plenary meetings
  - FATF may also apply Recommendation 21, which calls for financial institutions to give special attention to business relations and transactions with persons, companies and financial institutions domiciled in the non-complying country.
  - Then, as a final measure, FATF may suspend the membership of the country in question.

3. Reviewing money laundering trends and countermeasures ("Typologies" exercise)
   - FATF members gather information on money laundering trends in an effort to ensure that its Recommendations remain up to date.

FATF- Objectives (cont.)

- Since its creation in 1989, FATF has been working under five-year mandates.

- FATF members agreed that the organization would continue to operate until December 2012, subject to renewal.

Financial Action Task Force 40 Recommendations

- The combined 40 + 9 Recommendations have become the world's blueprint for effective national and international AML and CTF
  - The criminal justice system and law enforcement.
  - The financial system and its regulation.
  - International cooperation.
- The most important changes made to the Recommendations were in 2003
  - Expanded coverage to include terrorist financing
  - Widened the categories of business that should be covered by national laws, including **real estate agents, precious metals dealers, accountants, lawyers and trust services providers**.
  - Specified compliance procedures on issues such as customer identification and due diligence, including enhanced identification measures for higher-risk customers and transactions.
  - Adopted a clearer definition of money laundering predicate offenses.
  - Encouraged prohibition of so-called "shell banks," typically set up in offshore secrecy havens and consisting of little more than nameplates and mailboxes, and urged improved transparency of legal persons and arrangements.
  - Included stronger safeguards, notably regarding international cooperation in, for example, terrorist financing investigations.

Some highlights of the 40 Recommendations are:

- **Designated Categories of Offenses**
  - **For the first time crimes were specified that would serve as ML predicates. Trying to conceal them through financial subterfuge would constitute criminal money laundering.**
- **Knowledge and Criminal Liability**
  - **Knowledge maybe inferred from objective factual circumstances. “willful blindness”**
- **Expanded Coverage of Industries**
  - **Casinos**
  - **Real Estate**
  - **Dealers in precious metals**
  - **Lawyers, notaries, accountants**
  - **Trust and Company Service providers (providing transactions for clients**

Some highlights of the 40 Recommendations are:

- Beneficial Ownership
  - Transparency – verify information or don't open acct.
  - Beneficial Owner – natural person who exercises ultimate control
- CDD – Customer Due Diligence
  - ID customer and Verify.
  - ID beneficial owner
  - ID purpose and nature of business relationship
  - Conduct ongoing due diligence
- CDD on PEPs and Correspondent Accounts
  - EDD, on correspondent accts
  - EDD on PEP's – politically exposed persons.

Some highlights of the 40 Recommendations are:

- Accounts in Anonymous of Fictitious Names
  - Recommend not to open account.
- Shell Banks
  - Recommend not to open account.
- CTR
  - Countries should require CTR system
- International Cooperation
  - Countries should rapidly provide the widest possible range of mutual legal assistance n ML and TF investigations.

FATF Guidance on Dismantling Terrorist Financing and "Special Recommendations"

- FATF members should commit to:
  - Implement relevant UN instruments regarding TF
  - Criminalize TF/Terrorist acts and terror organizations
    - "willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used — or with the knowledge that they are to be used — (a) to carry out a terrorist act(s); (b) by a terrorist organization; or (c) by an individual terrorist."
    - "should extend to any funds whether from a legitimate or illegitimate source." These offenses, the note says, "should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s)."
    - "It should also be an offense to attempt to commit the offense of terrorist financing," the note says. Yet it asserts that "criminalizing terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation."
    - "terrorist financing offenses should be predicate offenses for money laundering,"
  - Freeze funds of terrorists
  - Report suspicious transactions linked to terror.
  - Provide assistance to other LEAs.
  - Impose AML requirements on alternative remittance systems

FATF Guidance on Dismantling Terrorist Financing and "Special Recommendations"

- Strengthen customer ID measures.
- Ensure entities, non profit orgs aren't used for TF
  - Maintain and be able to present full program budgets that account for all expenses.
  - Conduct independent internal audits and external field audits, the latter to ensure funds are being used for intended purposes.
  - Identify every member of the board of directors and formalize the process by which they are elected, appointed and terminated
- Special Recommendation Nine, calls on countries to stop cross-border movements of currency and monetary instruments related to terrorist financing and money laundering and to confiscate such funds. It also calls for enhanced information sharing between countries on the movement of illicit cash related to money laundering and terrorist financing.

FATF and Non-Cooperative Countries

- FATF had a practice of “naming and shaming” countries

- Currently FATF identifies jurisdictions having deficiencies in their AML/CFT regimes.
  - 4 Broad categories of evaluation
    - Loopholes in financial regulations
    - Obstacles raised by other regulatory requirements
    - Obstacles to international cooperation
    - Inadequate resources for preventing or detecting money laundering activities.

The Basel Committee on Banking Supervision

- The Basel Committee on Banking Supervision, established in 1974 by the central bank governors of the G-10 countries.
- Promotes sound supervisory standards worldwide exclusively to central banks and international organizations.
  - Ensure that banks have procedures in place to avoid involvement with drug traders and other criminals.
  - 1988 Statement of Principals
    - CID - KYC
    - Compliance with laws
    - High ethics
    - Full cooperation with national law enforcement
    - Staff training
    - Record keeping and audits

The Basel Committee on Banking Supervision

- 1997 issues a paper on KYC
  - Banks should establish ID and monitor accounts
  - Numbered accts must have KYC tests
  - KYC includes customer background. Country of origin, business activity and other risk indicators
  - Private banking must have KYC
  - Businesses have full vetting
  - Avoid anonymity
  - Conduct periodic training
  - Internal Audits
  - Monitor high-risk accounts
  - Ensure bank is complying with KYC procedures

European Union Directives on Money Laundering

- Directives have the force of law.
- First directive
  - Requires member nations to have ML laws.
- Second directive
  - Requires stricter AML laws
    - Expands first directive beyond drug-related crimes
    - MSB's were included
    - Knowledge of criminal activity can be inferred.
    - Better definition of money laundering
  - Widened to apply to gate-keepers. Auditors accountants, tax advisers, real estate agents legal professionals.
    - Certain persons, including lawyers when they participate in the movement of money for clients, were required to report to authorities any fact that might indicate money laundering

European Union Directives on Money Laundering

- Third directive
  - Adopted much of FATF 40 requirements
  - ML and TF two separate crimes.
  - CID and SARS to trusts, insurance intermediaries selling of goods for cash.
  - Detailed risk-based approach to CDD.
  - Protected employees who report suspicion
  - Members must keep statistics.
  - All financial institutions must ID and verify beneficial owners.
- Defines PEPs "Politically exposed persons" means natural persons who are or have been entrusted with prominent public functions and the immediate family members, or individuals known to be close associates, of such persons.
  - Third directive applies to Credit institutions, Financial institutions, Auditors, accountants, legal professionals. Trust and company service providers, RE agents. High value goods sellers and casinos.

Regional and Other International Initiatives

- Regional FATF-Style Bodies and FATF Associate Members
  - Asia/Pacific Group on Money Laundering (APG)
  - Caribbean Financial Action Task Force (CFATF)
  - Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV).
  - Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).
  - Eurasian Group (EAG).
  - Financial Action Task Force of South America againstMoney Laundering (GAFISUD – Grupo de Acción Financiera de Sudamérica)
  - Intergovernmental Action Group against Money-Laundering in West Africa (GIABA – GroupeIntergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Quest)
  - Middle East and North Africa Financial Action Task Force (MENAFATF)

Other Anti-Money Laundering Initiatives

- ORGANIZATION OF AMERICAN STATES: INTER-AMERICAN DRUG ABUSE CONTROL COMMISSION
  - In May 1992, the Organization of American States (OAS) became the first permanent international body to reach an agreement on the details of model legislation aimed specifically at dealing with money laundering.
  - Serves as the Western Hemisphere's policy forum on all aspects of the drug problem.
  - Fosters multilateral cooperation on drug issues in the Americas.
  - Executes action programs to strengthen the capacity of member states to prevent and treat drug abuse, to combat production and trafficking of illicit drugs; and to deny traffickers their ill-gotten gains.
  - **153 Compliance Standards for Anti-Money Laundering and Combating the Financing of Terrorism**
  - Promotes drug-related research, information exchange, specialized training and technical assistance.
  - Develops and recommends minimum standards for drug-related legislation; treatment; the measurement of both drug consumption and the cost of drugs to society; and drug-control measures, among others.

Other Anti-Money Laundering Initiatives

- Egmont Group of Financial Intelligence Units
  - In 1995, a number of national financial intelligence units (FIUs) began working together in an informal organization known as the Egmont Group
  - The goal of the group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field

Other Anti-Money Laundering Initiatives

- The Wolfsberg Group
  - The Wolfsberg Group is an association of 11 global banks that aims to develop financial services industry standards and related products for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.
    - Due diligence should be risk-based, depending on the location, type of business, ownership, customer base, regulatory status and AML controls of the correspondent banking client or business
    - An institution should not offer its products or services to a shell bank

Other Anti-Money Laundering Initiatives

- The World Bank and the International Monetary Fund
  - Support FATF and require countries that benefit from them must have effective ML programs.
  - Concentrating on money laundering over other forms of financial abuse.
  - Helping to strengthen “financial supervision and regulation” in countries.
  - More closely interacting with the OECD and the Basel Committee on Banking Supervision.
  - Insisting on the application of international AML standards in countries that ask for financial assistance

Other International Organizations

- African Development Bank.
- Asia Development Bank.
- The Commonwealth Secretariat.
- European Bank for Reconstruction and Development (EBRD).
- European Central Bank (ECB).
- Europol. Inter-American Development Bank (IADB).
- Interpol.
- International Organization of Securities Commissions (IOSCO).
- Offshore Group of Banking Supervisors (OGBS).
- World Customs Organization (WCO).

Key U.S. Legislative and Regulatory Initiatives Applied to Transactions Internationally

- USA Patriot Act
  - Section 311
    - U.S. Treasury Department has the authority to apply graduated, proportionate measures against a foreign jurisdiction, a foreign financial institution, a type of international transaction or a type of account that the Treasury Secretary determines to be a “primary money laundering concern.
    - Once identified Treasury can require US financial institutions to follow any or all of the following
      - Keep records/ or file reports
      - Obtain beneficial ownership information.
      - Obtain information oh foreign banks “payable-through accts”
      - Obtain information on correspondent accounts
      - Close certain payable-through or correspondent accounts.

Key U.S. Legislative and Regulatory Initiatives Applied to Transactions Internationally

- USA Patriot Act
  - Section 312
    - Require DD or EDD on foreign correspondent and private banking accounts for non-us persons. EDD when...
      - EDD if offshore banking license institutions,
      - EDD if license issued by a foreign country which is designated as non-cooperative.
      - EDD if license issued by a foreign country that has been designated by the Us as warranting special measures.
      - EDD must include
        - » Determine whether correspondent account is used by other banks with correspondent accounts.
        - » Determine identify of each owner of foreign bank who has a ten percent or more vote.
        - » Obtaining information relating to the foreign bank's AML program.
          - Monitoring transactions in and out of the correspondent account in a manner reasonably designed to detect possible money laundering and suspicious activity.
          - Obtaining information about the correspondent account that is being used as a payable-through account.
    - Private banking accounts
      - Take reasonable steps to identify nominal and beneficial owners
      - Determine if owner is a Senior foreign political figure
      - Determine source of funds in the account
      - Bank activity is consistent with information provided.

Key U.S. Legislative and Regulatory Initiatives Applied to Transactions Internationally

- Section 313 –
  - Prohibits US banks and security brokers/dealers from maintaining correspondent accounts for foreign unregulated “shell” banks that have no physical presence.
  - Also must ensure foreign banks with correspondent accounts do not permit access to the accounts referred above.

Key U.S. Legislative and Regulatory Initiatives Applied to Transactions Internationally

- Section 319(a)
  - Forfeiture from U.S. Correspondent - In situations where funds have been deposited with a foreign bank, this section permits the U.S. Government to seize funds in the same amount from a correspondent bank account in the U.S. that has been opened and maintained for the foreign bank. The U.S. Government is not required to trace the funds, as they are deemed to have been deposited into the correspondent account. However, the owner of the funds may contest the seizure order
- Section 319(b)
  - Fed banking agency to require financial institution to produce, within 120 hrs, records related to institutions aml compliance.

The Reach of the U.S. Criminal Money Laundering and Civil Forfeiture Laws

- Civil Forfeiture Laws only apply if the property involved in the financial transaction at issue represents the proceeds of at least one designated underlying crime.

- This money laundering law also reaches foreign individuals and foreign financial institutions if the financial transaction occurs in whole or in part in the U.S. or if the foreign financial institution maintains a bank account at a U.S. financial institution.

Office of Foreign Assets Control

- OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy

Chapter 4

- anti-money laundering compliance program
  - Risk-based -As money laundering risks increase, stronger controls are necessary.
  - Risk based is better because it is
    - Flexible – tailor to specific needs
    - Effective – ‘ground truth’
    - Proportionate –minimize adverse impact of anti-money laundering procedures.

What Risks Do Your Customers Pose?

- Levels of Risk
  - Prohibited
    - Do not do business with …
      - Countries subject to economic sanctions.
      - Designated State sponsors of terrorism
      - Shell banks.
  - High-Risk
    - More stringent controls
      - Countries noted for corruption
      - Drug trafficking countries.
      - PEPs
      - Correspondent banking and private banking
  - Medium-Risk
    - Merit additional scrutiny
  - Low-or Standard-Risk

A risk-scoring model

- Generally uses numeric values assigned to each of the following. Typically between 1 and 10. lowest risk to highest risk.

  Based on….

  - Geography – Known for ML? Sponsors of TF. Consider the organizations, FATF etc., involved with and ML laws.
  - Customer Type – Casino, individual travel agent. Etc.,
  - Product and Services – checking acct. Pay through accts., money transmitter, no clear primary beneficiary.
- High-risk does not mean no relationship – it may mean greater controls.

Elements of an AML program

- A system of internal policies, procedures and controls;
- A designated compliance officer with day-to-day oversight over the AML program;
- An ongoing employee training program; and
- An independent audit function to test the AML program.

AML compliance program

- Identify high-risk operations (products, services, customers, and geographic locations); provide for periodic updates to the institution's risk profile; and provide for an AML compliance program tailored to manage risks.
- Inform the board of directors (or a committee of the board) and senior management of compliance initiatives, known compliance deficiencies, suspicious transaction reports filed and corrective action taken.
- Assign clear accountability to persons for performance of duties under the anti-money laundering program.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory requirements and recommendations for anti-money laundering compliance.
- Provide for periodic review as well as timely updates to implement changes in regulations. Generally, this should be done at least on an annual basis.

AML compliance program

- Implement risk-based CDD policies, procedures and processes.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity. (Institutions should consider centralizing their own review and report-filing functions.)
- Provide for dual controls and segregation of duties. Employees who complete the reporting forms should not also be responsible for filing the reports or granting the exemptions.
- Comply with all recordkeeping requirements, including retention and retrieval of records.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of activity, such as for large currency or large transaction reporting.

AML compliance program

- Provide for adequate supervision of employees who handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the anti-money laundering laws, including implementing regulations.
- Train employees to be aware of their responsibilities under anti-money laundering laws, regulations and internal policy guidelines.
- Incorporate anti-money laundering compliance into the job descriptions and performance evaluations of appropriate personnel.
- Develop and implement screening programs to ensure high standards when hiring employees. Implement sanctions for employees who consistently fail to perform in accordance with an AML framework.
- Develop and implement program testing to assess the effectiveness of the program's implementation and execution of its requirements. This is separate from the independent audit requirement, but serves a similar purpose — to assess the effectiveness of the program

Compliance Officer

- responsible for designing and implementing the program,
- making necessary changes and disseminating information about the program's successes and failures to key staff members,
- constructing anti-money laundering-related content for staff training programs
- staying current on legal and regulatory developments in the field.

The department can be organized into subgroups – an example

- The Investigations Group – monitors alerts generated on customer transactions.
- Line of Business Support Group – Assigns risk
- The Program Oversight Group – performs internal audits

Training

- Who to train? Customer contact staff, back Office personnel, audit and compliance staff, aml compliance staff, senior management and board of directors.
- What to train? Legal framework, penalties, what to do in the event of a suspicious client, how to respond to customers who want to structure. CIP verification and CDD polities, record keeping requirement, etc..
- How to train?
- When to train?
- Where to Train?

Audit

- The audit must be independent
- individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors
- Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable

Audit

- Address the adequacy of AML risk assessment.
- Examine the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the institution's AML policies, procedures and processes.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations).
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program.

Audit

- Evaluate the system's ability to identify unusual activity by:
  - Reviewing policies, procedures, and processes for suspicious activity monitoring.
  - Evaluating the system's methodology for establishing and analyzing expected activity or filtering criteria.
  - Evaluating the system's ability to generate monitoring reports.
  - Determining whether the system's filtering criteria are reasonable.
- If an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets, tapes

Audit

- Review Suspicious Transaction Reporting (STR) systems,
  - which should include an evaluation of the research and referral of unusual transactions.
  - Testing should include a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines (e.g., legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.
- Assess the effectiveness of the institution's policy for reviewing accounts that generate multiple suspicious transaction report filings.
- Assess the adequacy of recordkeeping.
- Track previously identified deficiencies and ensure management corrects them.
- Decide whether the audit's overall coverage and frequency are appropriate to the risk profile of the organization.
- Consider whether the board was responsive to earlier audit findings.

Audit

- Determine the adequacy of the following, as they relate to the training program and materials:
  - The importance the board and senior management place on ongoing education, training and compliance.
  - Employee accountability for ensuring AML compliance.
  - Comprehensiveness of training, in view of specific risks of individual business lines.
  - Training of personnel from all applicable areas of the institution.
  - Frequency of training.
  - Coverage of internal policies, procedures, processes and new rules and regulations.
  - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
  - Sanctions for noncompliance with internal policies and regulatory requirements.

Compliance Culture and Senior Management's Role

- Ultimate responsibility for the AML compliance program rests with the board of directors
- Senior management must show its commitment to compliance by:
  - Establishing a strong compliance plan that is approved by the board of directors and is fully implemented.
  - Insisting that it be kept informed of compliance efforts, audit reports and any compliance failures, with corrective measures instituted.
  - Communicating compliance expectations to the institution personnel.
  - Including regulatory compliance within the job descriptions and job performance evaluations of institution personnel.
  - Implementing procedures, processes and controls to ensure compliance with the AML program.
  - Conditioning employment on regulatory compliance

Customer Due Diligence
(best way to prevent money laundering)

- Full identification of customer and business entities, including source of funds and wealth when appropriate.
- Development of transaction and activity profiles of each customer's anticipated activity.
- Definition and acceptance of the customer in the context of specific products and services.
- Assessment and grading of risks that the customer or the account present.
- Account and transaction monitoring based on the risks presented.
- Investigation and examination of unusual customer or account activity.
- Documentation of findings.

Account Opening, Customer Identification and Verification

- A sound CDD program should have reliable customer identification and account opening procedures.
  - Legal name and any other names used (such as maiden name).
  - Correct permanent address (the full address should be obtained; a postal box number is usually not sufficient).
  - Telephone and fax numbers and e-mail address.
  - Date and place of birth.
  - Nationality.
  - Occupation, position held and name of employer.
  - An official personal identification number or other unique identifier contained in an unexpired, official, government-issued document (e.g., passport, identification card, residence permit, driver's license) that bears a photograph of the customer.
  - Type of account and nature of the banking relationship.
  - Signature.

Account Opening, Customer Identification and Verification

- Confirming the date of birth from an official document (e.g., birth certificate, passport, identity card).
- Confirming the permanent address using an official document (e.g., utility bill, tax assessment, bank statement, letter from a public authority).
- Contacting the customer by telephone, letter or e-mail to verify the information supplied after an account has been opened (a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation).
- Confirming the validity of the official documentation either by physical verification of the original or through certification by an authorized person (e.g., embassy official).

Account Opening, Customer Identification and Verification

- For corporate entities (e.g., corporations and partnerships), the following information should be obtained
  - Name of institution.
  - Principal place of its business operations.
  - Mailing address.
  - Names of primary contact people or those authorized to use the account.
  - Contact people's telephone and fax numbers.
  - Some form of official identification number, if available (e.g., tax identification number).
  - The original or certified copy of the Certificate of Incorporation, Memorandum and Articles of Association.
  - The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account, including beneficial owners.
  - Nature and purpose of business, and its legitimacy

Account Opening, Customer Identification and Verification

- The institution should verify this information by at least one of the following methods:
  - For established corporate entities, review a copy of the latest report and accounts (audited, if available).
  - Conduct an inquiry by a business information service, or obtain an undertaking from a reputable firm of lawyers or accountants (or, in some countries, verifying officers) confirming the documents submitted. Undertake a company search or other commercial inquiries to see that the institution has not been, or is not in the process of being, dissolved or terminated.
  - Use an independent information verification process, such as by accessing public and private databases.
  - Obtain prior bank references.
  - Visit the corporate entity, where practical.
  - Contact the corporate entity by telephone, mail or e-mail

Account Opening, Customer Identification and Verification

- A written Customer Identification Program (CIP) must be included within the institution's AML compliance program and must include, at a minimum, policies, procedures and processes for the following
  - Identifying information required to be obtained (including name, address, taxpayer identification number and, for individuals, date of birth), and riskbased identity verification procedures (including procedures that address situations in which verification is not possible).
  - Complying with recordkeeping requirements.
  - Checking new accounts against prescribed government lists, if applicable

Account Opening, Customer Identification and Verification

- A written Customer Identification Program (CIP) must include (cont.)
  - Providing adequate notice about customer identification requirements.
  - Covering the institution's reliance on other financial institutions or third parties, if applicable.
  - Determining whether and when suspicious transaction reports should be filed.
  - Conducting a risk analysis of customers for account opening purposes, which consider the types of accounts offered, methods of account opening, and the institution's size, location and customer base.
  - Opening new accounts for existing customers.
  - Obtaining the approval of the board of directors, either separately for the CIP or as part of the AML compliance program.
  - Conducting audit and training programs to ensure that the CIP is adequately incorporated.
  - Verifying that all new accounts are checked on a timely basis against prescribed government lists for suspected terrorists or terrorist organizations.

Name Checking Lists

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons list. Updated often
  - it contains hundreds of names of individuals and businesses the U.S. government considers to be terrorists or international narcotics traffickers and others that are covered by U.S. foreign policy and trade sanctions

Consolidated CDD (eliminate information silos)

- According to the Basel Committee, a global risk management program for CDD should incorporate consistent identification and monitoring of customer accounts globally across business lines and geographical locations, as well as oversight at the parent level, in order to capture instances and patterns of unusual transactions that might otherwise go undetected.

Know Your Employee

- A Know Your Employee (KYE) -
  - program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity
- Once the person is hired, an ongoing approach to screening should be considered for specific positions, as circumstances change, or as needed for a comprehensive review of departmental staff over a period of time. Management should also have policies that address what to do when a screening uncovers information contrary to what the applicant or employee provided, according to the FDIC.

Suspicious or Unusual Transaction Monitoring and Reporting

- Some of the reports include:
  - Daily cash activity in excess of the country's reporting threshold.
  - Daily cash activity just below the country's reporting threshold (to identify possible structuring).
  - Cash activity aggregated over a period of time (e.g., individual transactions over a certain amount, or totaling more than a certain amount over a 30-day period) to identify possible structuring.
  - Wire transfer reports/logs (with filters using amount and geographical factors).
  - Monetary instrument logs/reports.
  - Check kiting/drawing on uncollected funds (significant debit/credit flows).
  - Significant change reports.
  - New account activity reports.

Suspicious or Unusual Transaction Monitoring and Reporting

- Typical suspicious or unusual transaction reporting process within a financial institution includes
  - Procedures to identify potential suspicious transactions or activity.
  - A formal evaluation of each instance, and continuation, of unusual transactions or activity.
  - Documentation of the suspicious transaction reporting decision, whether or not filed with the authorities.
  - Procedures to periodically notify senior management or the board of directors of suspicious transaction filings.
  - Employee training on detecting suspicious transactions or activity.

Red Flags or Indicators of Money Laundering

- **ATM Usage:**
  - Launderers can use an account in the U.S. to deposit funds within the U.S. and have another person withdraw them outside the country.
  - Domestic terrorists might find ATMs convenient to access accounts as they travel.
  - Deposit accounts with multiple access devices might be indicators of illegal abuse of ATMs.

Red Flags or Indicators of Money Laundering

- **Moving Customers:**
  - A customer who moves frequently could be suspicious, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal

Red Flags or Indicators of Money Laundering

- **Opening Deposits or Investments:**
  - Ask new customers about sources of funds,
  - when appropriate, institutions should consider determining the background of customer's first transaction.
  - Wire transfer from outside the country, monetary instruments and, of course, large cash transactions.

Red Flags or Indicators of Money Laundering

- **Out-of-Market Windfalls**
  - Pay attention to one whose address is far from your institution.
  - Do not be persuaded by sales personnel who might follow a “no questions asked” philosophy of taking in new business.

Red Flags or Indicators of Money Laundering

- **Credit balances:**
  - Large or frequent credit balances may also be red flags for money laundering.
  - Institutions should consider periodic evaluation of their credit products for unusual overpayments.

Red Flags or Indicators of Money Laundering

- **Common addresses, phone numbers, IP addresses and other data:**
  - unrelated customers who share street or IP addresses, or who have the same phone number or email account, could be using their accounts for suspicious or fraudulent purposes.
  - Customers who change their information after opening their accounts to common locations may be especially suspicious.
  - Institutions should consider evaluation of customers who have these common data characteristics

Suspicious Customer Behavior

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses your record-keeping or reporting requirements with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required recordkeeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be reported.
- Customer suggests paying a gratuity to an employee.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.

Suspicious Customer Behavior

- Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income.
- Customer makes large cash deposit without having counted the cash.
- Customer frequently exchanges small bills for large bills.
- Customer's cash deposits often contain counterfeit bills or musty or extremely dirty bills.
- Customer, who is a student, uncharacteristically transfers or exchanges large sums of money.
- Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances.

Suspicious Customer Behavior

- Transaction involves offshore institutions whose names resemble those of well-known legitimate financial institutions.
- Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map.
- Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney.
- Customer indulges in foreign exchange transactions/ currency swaps without caring about the margins.
- Customer submits account documentation showing an unclear ownership structure.

Suspicious Customer Identification Circumstances

- Customer furnishes unusual or suspicious identification documents or declines to produce originals for verification.
- Customer is unwilling to provide personal background information when opening an account.
- Customer tries to open an account without identification, references or complete local address.
- Customer's permanent address is outside of the institution's service area.
- Customer's home or business telephone is disconnected.
- Customer does not wish a statement of his account or any mail sent to him.
- Customer asks many questions about how the financial institution disseminates information about the identification of its customers.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.
- Customer provides no record of past or present employment on a loan application.
- Customer claims to be a law enforcement agent conducting an undercover operation when there are no valid indicators to support that claim.

Suspicious Cash Transactions

- Customer comes in with another customer and they go to different tellers to conduct currency transactions under the reporting threshold. Customer makes large cash deposit containing many larger denomination bills. Customer opens several accounts in one or more names, and then makes several cash deposits under the reporting threshold.
- Customer withdraws cash in amounts under the reporting threshold.
- Customer withdraws cash from one of his accounts and deposits the cash into another account the customer owns.
- Customer conducts unusual cash transactions through night deposit boxes, especially large sums that are not consistent with the customer's business.
- Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason, or for a business that generally does not generate large amounts of cash.
- Customer conducts large cash transactions at different branches on the same day, or coordinates others to do so in his behalf.
- Customer deposits cash into several accounts in amounts below the reporting threshold and then consolidates the funds into one account and wire transfers them abroad.
- Customer attempts to take back a portion of a cash deposit that exceeds the reporting threshold after learning that a currency transaction report will otherwise be filed.
- Customer conducts several cash deposits below the reporting threshold at ATMs.
- Corporate account has deposits or withdrawals primarily in cash, rather than checks.
- Customer frequently deposits large sums of cash wrapped in currency straps.

Suspicious Non-Cash Deposits

- Customer deposits a large number of traveler's checks, often in the same denominations and in sequence.
- Customer deposits large numbers of consecutively numbered money orders.
- Customer deposits checks and/or money orders that are not consistent with the stated purpose of the account or nature of business.
- Customer deposits a large number of third party checks.
- Funds withdrawn from the accounts are not consistent with the normal business or personal activity of the account holder or include transfers to suspicious international jurisdictions.
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

Suspicious Wire Transfer Transactions

- Non-accountholder sends wire transfer with funds that include numerous monetary instruments, each in an amount under the reporting threshold.
- An incoming wire transfer has instructions to convert the funds to cashier's checks and to mail them to a non-accountholder.
- A wire transfer directs large sums to secrecy havens.
- An incoming wire transfer, followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party.
- An increase in international wire transfer activity in an account with no history of such activity or where the stated business of the customer does not warrant it.
- Customer frequently shifts purported international profits by wire transfer out of the country.
- Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country.
- Customer deposits bearer instruments followed by instructions to wire the funds to a third party.
- Account in the name of a currency exchange house receives wire transfers or cash deposits under the reporting threshold.

Suspicious Safe Deposit Box Activity

- Customer spends an unusual amount of time in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash.
- Customer often visits the safe deposit box area immediately before making cash deposits of sums under the reporting threshold.
- Customer rents multiple safe deposit boxes.

Suspicious Activity in Credit Transactions

- A customer's financial statement makes representations that do not conform to accounting principles.
- A transaction is made to appear more complicated than it needs to be by use of impressive but nonsensical terms such as emission rate, prime bank notes, standby commitment, arbitrage or hedge contracts.
- Customer requests loans either made to offshore companies or secured by obligations of offshore banks.
- Customer suddenly pays off a large problem loan with no plausible explanation as to the source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.
- Customer collateralizes a loan with cash deposits.
- Customer uses cash collateral located offshore to obtain a loan.
- Customer's loan proceeds are unexpectedly transferred offshore.

Suspicious Commercial Account Activity

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- Retail business that provides check-cashing services does not make withdrawals of cash against check deposits, possibly indicating that it has another source of cash.
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.
- Corporate account shows little or no regular, periodic activity.
- A transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral.

Suspicious Trade Financing Transactions

- Customer seeks trade financing on the export or import of commodities whose stated prices are substantially
- more or less than those in a similar market situation or environment.
- Customer makes changes to a letter of credit beneficiary just before payment is to be made.
- Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary’s stated location.
- Customer’s standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or designates unusual beneficiaries.
- Letter of Credit is inconsistent with customer’s business.
- Letter of Credit covers goods that have little demand in importer’s country.
- Letter of Credit covers goods that are rarely if ever produced in the exporter's country.
- Documents arrive without title documents.
- Letter of Credit is received from countries with a high risk for money laundering.
- Commodities are shipped through one or more jurisdictions for no apparent economic or logistical reason.
- Transaction involves the use of repeatedly amended or frequently extended letters of credit.
- Size of the shipment appears inconsistent with the regular volume of business of the importer or of the exporter.

Suspicious Investment Activity

- Customer uses an investment account as a pass through vehicle to wire funds to off-shore locations.
- Investor seems uninterested in the usual decisions to be made about investment accounts, such as fees or the suitability of the investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions.
- Customer deposits cash, money orders, traveler's checks or cashier's checks in amounts under the reporting threshold to fund an investment account.
- Customer cashes out annuities during the "free look" period or surrenders the annuities early.

Suspicious Employee Activity

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee is involved in an excessive number of unresolved exceptions.
- Employee lives a lavish lifestyle that could not be supported by his or her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy
- Employee uses company resources to further private interests.
- Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed.
- Employee avoids taking periodic vacations

Suspicious Activity in a Money Remitter/ Currency Exchange House Setting

- Unusual use of money orders, traveler's checks or funds transfers.
- Two or more persons working together in transactions.
- Transaction altered to avoid filing a Currency Transaction Report (CTR).
- Customer comes in frequently to purchase less than $3,000 in instruments each time (or the local threshold).
- Transaction altered to avoid completion of record of funds transfer, money order or traveler's checks of $3,000 or more (or the local threshold).
- Same person uses multiple locations in a short time period.
- Two or more persons use the same identification.
- One person uses multiple identification documents.

Suspicious Activity in an Insurance Company Setting

- Cash payments on insurance policies.
- Refunds requested during a policy's "legal cancellation period."
- Policy premiums paid from abroad, especially from an offshore financial center.
- A policy calling for the periodic payment of premiums in large amounts.
- Changing the named beneficiary of a policy to a person with no clear relationship to the policyholder.
- Lack of concern for significant tax or other penalties assessed when canceling a policy.
- Redemption of insurance bonds originally subscribed to by an individual in one country by a business entity in another country.

Suspicious Activity in a Broker-Dealer Setting

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence.)
- The customer's account shows an unexplained high level of activity with very low levels of securities transactions.

Suspicious Activity Indicators of Black Market Peso Exchange Money Laundering Method

- Payment made in cash by a third party with no connection to the underlying transaction.
- Payment made by wire transfers from third parties unconnected to the underlying transaction.
- Payment made with checks, bank drafts or money orders not drawn on the account of the purchaser.

“potential indicators” that an institution or business is being abused by peso brokers:

- Structured currency deposits to individual checking accounts with multiple daily deposits to multiple accounts at different branches of the same bank on the same day.
- Consumer checking accounts which are used for a period of time and then become dormant.
- Personal checking accounts opened by foreign nationals who come to the bank together.
- Multiple accounts opened on the same day or held by the same foreign nationals at various banks.
- Increases in the frequency or amounts of currency deposits by U.S. business account holders who export to Colombia.

Electronic Anti-Money Laundering Solutions

- Financial institutions use technology to assist them in their AML goals:
  - Profiling system;
  - Large cash transaction reporting;
  - Recordkeeping;
  - Background checks;
  - Corporate “hot file”; Case management tracking system; and incident reporting database

Chapter 5

Conducting and responding to investigations

Law Enforcement Investigations

- Steps that law enforcement agencies should take
  - Follow the money
  - Identify the unlawful activity
  - Document the underlying activity and transactions
  - Review databases
  - Review public records
  - Review licensing and registration files
  - Analyze the financial transactions and account activity of the target
  - Review STRs
  - Conduct computer-based searches
  - In cross-border cases, seek international assistance,

Decision to Prosecute

- The institution has a criminal history.
- The institution has cooperated with the investigation.
- The institution discovered and self-reported the money laundering-related issues.
- The institution has had a comprehensive and effective AML program.
- The institution has taken timely and effective remedial action.
- There are civil remedies available that can serve as punishment.
- Deterring wrongdoing by others is needed and will be served by a prosecution.

Responding to a Law Enforcement Investigation

- respond quickly and completely to all requests
- the institution can attempt to narrow the request or can even seek to contest the request, or portions of the request, in court.
- However, under no circumstances should an institution ignore, defer or otherwise put aside or delay responding to a law enforcement inquiry or request for documents.

Responding to a Law Enforcement Investigation

- When confronted with a law enforcement inquiry, the financial institution needs to ensure that the appropriate senior management is informed..
- and that someone is designated as being responsible for monitoring all LEA requests,
- monitoring the progress …
- and keeping senior management informed…

Responding to a Law Enforcement Investigation

- consideration should be given to the retention of qualified, experienced legal counsel necessary.
- If the law enforcement inquiry is merely focused on a particular account or is only seeking to obtain financial evidence about a customer and there is no apparent wrongdoing by the institution, there is a less pressing need to obtain counsel
- the institution should conduct an inquiry of its own to determine the underlying facts, the institution's exposure and what steps, if any, the institution should take.

Summonses and Subpoenas

- the institution should have its senior management and/or counsel review the summons or subpoena.
- If there are no grounds for contesting the summons or subpoena, the institution should take all appropriate measures to comply with the summons or subpoena on a timely and complete basis.
- Also, the financial institution should not notify the customer who is being investigated
- If the government asks the bank to keep certain accounts open, such a request should be obtained in writing under proper letterhead and authority from the government

Search Warrants

- Call the financial institution's in-house or outside counsel.
- Review the warrant to understand its scope.
- Ask for and obtain a copy of the warrant.
- Ask for a copy of the affidavit that supports the search warrant. The agents are not obligated to provide a copy of the affidavit, but, if a financial institution is allowed to see the affidavit, the financial institution can learn more about the purpose of the investigation.
- Remain present while the agents record an inventory of all items they seize and remove from the premises.
- Keep track of the records taken by the agents.
- Ask for a copy of law enforcement's inventory of what they have seized.
- Write down the names and agency affiliations of the agents who conduct the search.

Orders to Restrain or Freeze Accounts or Assets

- the institution should obtain a copy of the order and should comply with it.
- Generally, the order is obtained based on a sworn affidavit, which is sometimes included with the order. If the affidavit is not part of the order, the financial institution can ask to see the affidavit, which should provide clues about why a customer's information is being requested

Monitoring the Institution's Response to a Law Enforcement Investigation

- All should be reviewed by senior management, an investigations group or counsel to determine how best to respond to the inquiry and to determine if the inquiry or the underlying activity might pose a risk to the institution
- Maintain a centralized control over all requests and responses
- This centralized record will also assist with regard to the institution's own internal investigation

Dealing with Investigators and Prosecutors

- the most effective strategy is to cooperate with investigators and prosecutors
- It is also important for the institution to try to learn how the investigators and prosecutors view the facts

Obtaining Counsel for the Investigation

- it is recommended that institutions hire or consult experienced outside legal counsel if confronted with a government investigation of the institution itself.

Notices to Employees

- employees should be informed of the investigation
- instructed not to produce corporate documents directly
- the institution will know what is being requested and what has been produced
- the institution can determine what, if any, requests should be contested

Media Relations

- If the facts are not on the institution's side, "no comment" may be the best response

Internal Investigations

- When?
- A report of examination from the regulators.
- Information from third parties, such as customers.
- Information derived from surveillance or monitoring systems.
- Information from employees or a company hotline.
- Receipt of a governmental subpoena or search warrant.
- Learning that government investigators are asking questions of institution employees, business associates, customers or even competitors.
- The filing of a civil lawsuit against the institution or a customer of the institution.

Closing the Account

- The legal basis for closing an account.
- The institution's stated policies and procedures for closing an account.
- How serious is the underlying conduct. If the conduct is serious and rises to the level where the account would ordinarily be closed, then the institution should consider closing the account.
- As stated above, if law enforcement requests the institution to keep the account open, the institution should request that the investigator or prosecutor make that request in writing on proper government agency letterhead with the appropriate authorized signature

Conducting the Investigation

- **Documents**
  - Unusually high monthly balances in comparison to known sources of income.
  - Unusually large deposits, deposits in round numbers or deposits in repeated amounts that are not attributable to legitimate sources of income.
  - Multiple deposits made under reportable thresholds.
  - The timing of deposits. This is particularly important when dates of illegal payments are known.
  - Checks written for unusually large amounts (in relation to the suspect's known practices).
  - A lack of account activity. This might indicate transactions in currency or the existence of other unknown bank account

Conducting the Investigation

- **Finding and Reviewing the Documents**
  - An institution should start by identifying an employee with knowledge of the institution's files, who will be in charge of retrieving documents for the institution.
  - A system must be put in place to ensure that all documents are located, whether they be in central files, department files, and even individual files.
  - In addition, copies of the same document in different hands should be retrieved

Conducting the Investigation

- **Organization of Documents**
  - The institution should ensure the integrity of original documents, while at the same time minimizing disruption to the institution's business.

Conducting the Investigation

- **Interviewing Employees**
  - it is important to interview all knowledgeable employees
- In addition, the institution - usually counsel - should prepare employees who expect to be interviewed by law enforcement investigators should debrief them after their interviews.

Conducting the Investigation

- **Attorney - Client Issues Applied to Entities and Individuals**
  - In an internal investigation, all parties should be aware that attorneys for the organization represent the entity
  - There may be major consequences if the interests of an entity and its employees diverge or conflict
  - In such cases, separate counsel may be required

Conducting the Investigation

- **Dissemination of a Written Report by Counsel**
  - the institution should take steps to not inadvertently waive the attorney-client privilege
  - Do not distributing the report to persons who should not receive it.
  - Every page of the report should contain a statement that it is confidential and is subject to the attorney-client privilege and work-product privilege
  - Copies of the report should be numbered
  - list of persons who are given copies to read should be maintained.
  - Persons obtaining the report should be instructed not to make notes on their copies

Exploiting the Internet for Money Laundering Investigations

- Page 265 to 270 …..Seriously, need we say more?

AML Cooperation Between Countries

- **International Money Laundering Information Network**
  - a clearinghouse of money laundering information for the benefit of national and international anti-money laundering agencies
  - United Nations Office on Drugs and Crimes (UNODC)
    - **AMLID: Anti-Money Laundering International Database -** A compendium and analysis of national AML laws and regulations, as well as information on national contact and authorities.
    - **Reference Data: Research and analysis, bibliography,** conventions, legal instruments and model laws
    - **Country Page: Includes full text of AML legislation** where available, and links to national FIUs.
    - **Calendar of Events: Chronological listing of training** events, conferences, seminars, workshops and other meetings in the AML field.
    - **Current Events: Current news of recent AML** initiatives.

AML Cooperation Between Countries

- **Mutual Legal Assistance Treaties –gateway 1**
  - provides a legal basis for transmitting evidence that can be used for prosecution and judicial proceedings
    - The central authority of the requesting country sends a "commission rogatoire"
    - The central authority that receives the request sends it to a local financial investigator
    - An investigator from the requesting country then visits the country where the information is sought
    - The investigator asks the central authority for permission to remove the evidence
    - The central authority sends the evidence to the requesting central authority

Financial Intelligence Units

- Generally, FIUs are agencies that receive reports of suspicious transactions from financial institutions - gateway 2
  - When establishing an FIU remember -
    - Objectives to be pursued by the establishment of the FIU need to be defined
    - The FIU must be given the means to successfully pursue these objectives
    - Care should be taken not to give the FIU more responsibilities than it can handle,
    - Overlapping functions should be avoided to the extent possible

Financial Intelligence Units

- Principles of FIUs from Edgemont group
  - An MOU
  - free exchange of information at the FIU level should be possible on the basis of reciprocity
  - Differences in the definition of offenses that fall under the competence of FIUs should not be an obstacle to free exchange of information at the FIU level

The Supervisory Channel

- Report on Sharing of Information between Jurisdictions in Connection with the Fight against Terrorism - 3rd gateway
  - cites the supervisory channel as the third official gateway.
  - It says that with regard to banking, information from supervisory agencies is normally of a general character and is designed to monitor the financial soundness of a banking group

FATF Recommendations on Cooperation Between Countries

- Recommendations 36 – 40 from the FATF's 40 Recommendations pertain specifically to the international aspects of money laundering and terrorist financing investigations.
- They deal with mutual legal assistance treaties, extradition, confiscation of assets and mechanisms to exchange information internationally.

– The end…..

Internal Policies, Procedures and Controls

- identify and understand the applicable laws and regulations
- The institution should then look at its own risk assessment and gauge its risk appetite
- Internal anti-money laundering policies should be established or approved by higher management or the board of directors, and should set the tone for the organization