The 10th Annual Banking Law Institute

Bank Secrecy Act and Anti-Money Laundering Compliance

Amy G. Rudnick
Partner

Minneapolis
April 5, 2013

Overview

- What is money laundering?
- The current highly-charged regulatory environment
- Key anti-money laundering laws and regulations
- What is on the horizon: Customer due diligence
- Recent criminal and regulatory enforcement actions
- Key compliance breakdowns that can lead to enforcement actions and how to steer clear of them

2

What is Money Laundering?

- Money laundering is the process by which a person conceals the existence, nature or source of the proceeds of illegal activity and disguises them to make them appear legitimate.
- Banks also need to be concerned with “reverse money laundering,” using legal proceeds for unlawful activities, *e.g.*, terrorist financing through charities.

3

Why Money Laundering?

- Money laundering sustains all types of criminal activity that generate proceeds – drug trafficking, alien smuggling, illegal gaming, political corruption, illegal arms sales, and all types of fraud.
- Money laundering also facilitates terrorism.
- Criminals launder funds to keep the enterprise growing and profitable, to diversify into “legal” businesses and, primarily, to enjoy the fruits of their labors – all under the radar screens of governmental authorities.
- It happens because crime pays. Criminals can bear the cost of laundering their proceeds and still turn an enormous profit.

4

The Government's Money Laundering Focus

- Drug trafficking, particularly with respect to Mexico
- Terrorism and terrorist financing
- Foreign public corruption
- Consumer fraud/Mortgage fraud
- Serious Bank Secrecy Act failings

5

The Current Regulatory Environment

- Since 9/11 and the passage of the USA PATRIOT Act, there have been waves of BSA/AML regulatory actions with ever-increasing civil money penalties and expensive and burdensome remedial measures.
- Recently, high-profile enforcement actions have resulted in enhanced Congressional scrutiny and pressure on the regulators to be rigorous and less gradual and measured in exercising their enforcement authority.
- Congress has asked the regulators and the Justice Department to consider taking action against bankers for compliance failures.
- The risk-based approach to BSA/AML compliance has become risky for financial institutions and their directors, officers and employees.
  - Examiners that were satisfied with a bank's BSA/AML program in one examination cycle may be hyper-critical in the next based on the sound practices that they are seeing at other financial institutions or the knowledge that they have gained as a result of enforcement actions.

6

Legal Requirements

- Three types of laws
  - Criminal
  - Forfeiture
  - Regulatory

Criminal Money Laundering Laws – 18 U.S.C. 1956 and 1957

- It is a crime to engage in virtually any type of financial transaction with the knowledge that the proceeds involved are the proceeds of *unlawful activity* if the government can prove that the proceeds were derived from a *specified unlawful activity*.
- *Unlawful Activity* – Generally any violation of criminal law – federal, state, local, or even foreign.
- *Specified Unlawful Activities*: There are over 200 specified unlawful activities – U.S. and foreign crimes.
- Knowledge includes the concept of willful blindness.
- Penalties
  - Up to 20 years in prison and fines up to $500,000 or double the amount of property involved, whichever is greater.
  - Civil or criminal forfeiture of any property involved in or traceable to the criminal proceeds (18 U.S.C. §§ 981 and 982).
  - The death penalty for banks (loss of charter or deposit insurance) following a money laundering conviction and an administrative hearing (12 U.S.C. § 1818(w)).

8

The Regulatory Requirements – The Bank Secrecy Act, as amended by the USA PATRIOT Act

- *Purpose of the BSA*: Provides authority to the Secretary of the Treasury to require reporting, recordkeeping and compliance program measures for financial institutions useful in criminal, tax and regulatory investigations and proceedings and to fight international terrorism.
- *Penalties*: Separate and stringent civil and criminal penalties, forfeiture, and the possibility of regulatory enforcement actions and charter or license revocation.
- Most criminal cases against financial institutions have been brought under the BSA, not under the money laundering statutes.

9

Sources of Authority for Enforcement of the BSA

- Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) – Bureau responsible for civil enforcement, issuance of regulations, and interpretations of the BSA, 31 U.S.C. 311 *et seq*. and 31 C.F.R. Chapter X (previously, 31 C.F.R. Part 103).
- The federal banking regulatory agencies enforce the BSA under delegations from FinCEN and also directly through parallel regulations under their own authority.
- The Department of Justice is responsible for criminal enforcement of the BSA and the money laundering statutes.

10

Principal Regulatory Requirements Applicable to Banks

- BSA/AML Compliance Program
- Customer Identification Program
- Enhanced Due Diligence procedures for foreign financial institution correspondent accounts and foreign private banking clients
- Suspicious Activity Reporting
- Currency Transaction Reporting
- International Transportation of Currency and Monetary Instrument Reporting
- Records of Cash Sales of Monetary Instruments
- Funds Transfer and Other Recordkeeping

11

Key BSA requirements which figure prominently in enforcement actions

- BSA/AML Compliance Programs
  - Four elements
    - Designated compliance officer
    - Written policies, procedures and internal controls to comply with the BSA and to prevent and detect money laundering and terrorist financing
    - Training of appropriate personnel
    - Independent testing (audit)
  - Risk assessments and the risk-based approach
    - Types of products, services and business lines, *e.g.*, foreign correspondent banking, RDC, services to non-customers
    - Types of customers – *e.g.*, NRAs and Money Services Businesses
    - Geographic locations – onshore and offshore

12

Suspicious Activity Reporting

- Banks, bank holding companies (BHCs) and their subsidiaries and certain other financial institutions must file Suspicious Activity Reports (SARs) electronically with FinCEN (generally within 30 days) if the financial institution knows, suspects or has reason to suspect that a transaction, transactions or *attempted* transactions by, at or through the financial institution that aggregate to $5,000 or more –
  - Involve money laundering or funds derived from illegal activity;
  - Are designed to evade the BSA, including structuring; or
  - Have no business or apparent lawful purpose or are not the sort of transactions in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation.

13

Suspicious Activity Reporting

- Banks, BHCs and their subsidiaries also must file SARs to report –
  - Known and suspected violations of federal criminal law involving insider abuse against the bank or involving transactions through the bank regardless of amount; and
  - Known and suspected violations of federal criminal law (other than BSA or money laundering violations) against the bank or involving transactions through the bank aggregating to $5,000 where a possible suspect has been identified or $25,000 if a potential suspect has not been identified.
- SARs must be filed even if the government already knows about the criminal activity, *e.g.*, where a bank has received subpoenas and is in contact with law enforcement.

14

The Gag Rule

- It is a crime for a financial institution and its directors, officers, employees and agents to disclose a SAR or the existence of a SAR to any person except:
  - SARs may be disclosed to FinCEN or any state, federal or local law enforcement agency, or any federal or state regulatory that examines the bank for compliance with the Bank Secrecy Act;
  - SARS may be shared with the bank's BHC, head office or controlling company in the United States or outside the United States and within the bank's corporate organizational structure with U.S. affiliates that are subject to SAR requirements.
  - The underlying facts, transactions, and documents can be shared so long as the existence of a SAR is not disclosed.

15

The Gag Rule

- If a financial institution is subpoenaed or otherwise requested to disclose a SAR to anyone (other than FinCEN or an appropriate law enforcement or regulatory agency), the financial institution must decline to provide the information and must notify FinCEN and the bank's federal functional regulator.
- In connection with civil litigation, bank counsel must be diligent not to produce SARs or to provide any information indicating that SARs were (or were not) filed.
  - What do you do if a SAR or SAR information is inadvertently produced?
- *A customer never should be advised that a matter is being referred as potentially suspicious, that a SAR may be filed, or that a SAR has been filed. Tipping off is a crime.*

16

Safe Harbor Protection from Civil Liability

- Financial institutions and their directors, officers, employees and agents are protected from civil liability to any person for reporting suspicious activity and for not notifying any person identified in the SAR of the disclosure, *e.g.*, the bank is protected from actions based on a breach of privacy or defamation even if the suspicion turns out to be wrong.
- Applies to voluntary disclosures (*e.g.*, for transactions less than $5,000).
- Applies to any cause of action under state or federal law, including in any arbitration proceeding.
- There is no safe harbor from criminal liability.
  - After filing a SAR, the bank must decide whether continuing to do business with the customer could expose the bank to possible criminal liability under the money laundering statutes.
- The safe harbor also does not protect a bank from damages based on closing the account.

17

What is the Scope of the Safe Harbor?

- Does the safe harbor provide unqualified immunity from claims arising from the filing of a SAR or must there be a finding that a SAR was filed in good faith?
- Congress rejected including a good faith element in the statute to minimize legal challenges and promote reporting.
- Federal and state courts differ on this issue, however.
- The issue remains in flux given the U.S. Supreme Court's denial without opinion in November 2012 of the *Petition for a Writ of Certiorari* in *Cummings III v. Doughty*, which involved a Louisiana state court decision.
- *Best view:* The motivation for filing should not be an issue if the bank has a bona fide suspicion.

18

SAR Identification and Monitoring

- FinCEN and the bank regulators expect banks to assess the money laundering risks posed by their customers, products, services, transactions, and geographic markets, and to develop risk-based Customer Due Diligence procedures to assist in the identification and reporting of suspicious activity.
- FinCEN and the regulators also expect banks to put in place policies and procedures to identify suspicious activity as it occurs, to develop and implement risk-based back-end transaction monitoring systems, and to maintain effective reporting processes and systems as part of an effective BSA/AML program.

Failure to File SARs

- Failures to file SARs and tipping off could result in criminal penalties, including imprisonment and large fines, civil money penalties, and/or other regulatory enforcement action against a financial institution and the employees involved.

19

Advanced Notice of Proposed Rulemaking
Customer Due Diligence Requirements for Financial Institutions

- Issued by FinCEN on March 5, 2012.
- Solicited public comment on the development of a Customer Due Diligence (CDD) program regulation to clarify and strengthen existing regulatory requirements and supervisory expectations and establish a new requirement to identify and verify the identities of the beneficial owners of accountholders.
- Comment period closed in June 2012.
- Take-aways from comments and FinCEN Regional Roundtable Meetings.
- *Next steps*: Issuance of a Notice of Proposed Rulemaking with an opportunity for comment prior to the publication of any final rule.

20

Advanced Notice of Proposed Rulemaking
Customer Due Diligence Requirements for Financial Institutions

- Key CDD Program Elements
  - Initial CDD at account opening, including CIP;
  - Understanding the purpose and intended nature of the account and the expected type and volume of transactions to assess risk and identify and report suspicious activity;
  - Generally, identifying the beneficial owners of all customers and risk-based verification of identity; and
  - Ongoing monitoring of customer relationships and updating CDD based on risk or events.

21

Beneficial Ownership

- Definition under consideration for entities
  - Either:
    - (a) Each individual who directly or indirectly, through contract, arrangement, understanding, intermediary, tiered entity, or otherwise, owns more than a 25% of the equity interests in the entity; ***or***
    - (b) If no one satisfies (a), the individual who has at least as great an equity interest as any other individual; ***and***
  - The individual with greater responsibility than any other individual for managing or directing the entity's regular affairs.

22

Verifying Beneficial Ownership Information

- Two possible meanings for “verification”
  - Verifying the identity/existence of beneficial owners consistent with CIP requirements.
  - Verifying that a beneficial owner is a beneficial owner.

23

Regulatory and Criminal Enforcement Actions

- Different types of enforcement actions
  - Informal actions by the bank regulators (nonpublic)
    - Supervisory Letters
    - Memoranda of Understanding
  - Formal actions by the bank regulators (public)
    - Cease and Desist Orders (C&Ds)
    - Written Agreements
  - Civil Money Penalties (CMPs) by FinCEN or the bank regulators
  - Criminal Actions by the U.S. Department of Justice or State Prosecutors
    - Deferred Prosecution Agreements (DPAs)
    - Non-Prosecution Agreements (NPAs)
- There is authority for parallel or separate actions against individuals – directors, officers, and employees.

24

Interagency Statement of Enforcement on Bank Secrecy Act/Anti-Money Laundering Requirements

- Guides the bank regulators in determining the type of action to take if concerns are raised during an examination about an institution's BSA/AML program or compliance with other BSA requirements.
- Concerns can be expressed through informal discussions with the institution's management, formal discussions with the Board of Directors, Supervisory Letters to Management, examination findings, or other formal communications to the Board of Directors.
- Sets forth the circumstances where the agencies will take formal enforcement action, including issuing a C&D.

25

Interagency Statement of Enforcement on Bank Secrecy Act/Anti-Money Laundering Requirements

- Under the *Interagency Statement*, a C&D action must be initiated where an institution:
  - Fails to have a written BSA/AML Program or implement a Program that adequately covers the four required elements.
  - Has defects in one or more elements that indicate that the Program is not effective, *e.g.*, where the deficiencies are coupled with other aggravating factors, such as unreported highly suspicious activity, patterns of structuring, significant insider complicity, or systematic failures to file Currency Transaction Reports (CTRs) or SARs.

26

Interagency Statement of Enforcement on Bank Secrecy Act/Anti-Money Laundering Requirements

  - Fails to correct a serious defect that was reported previously as a problem to the Board of Directors or Senior Management in an exam report or other written supervisory communication as a matter that must be corrected.

- The regulators also will take formal or informal supervisory action for other types of BSA/AML concerns, including failures to file SARs that result from systemic breakdowns in polices or procedures or that involve a pattern or practice of noncompliance or a significant or egregious situation.
- *The Result:* Increased numbers of BSA/AML examination criticisms, including Matters Requiring Immediate Attention (MRIAs), Matters Requiring Attention (MRAs), Violations, and regulatory enforcement actions, including C&Ds, Written Agreements and MOUs.

27

Civil Money Penalties and Criminal Enforcement Actions

- Where there have been serious BSA/AML compliance program violations, especially breakdowns in internal controls coupled with other BSA violations, like failures to file SARs, FinCEN and the bank regulators will assess CMPs.

- In those cases where the deficiencies have involved drug trafficking, terrorist financing, fraud, or other egregious BSA violations, financial institutions also have been subject to criminal enforcement actions, including DPAs with the U.S. Department of Justice (DOJ) and the U.S. Attorney's Offices or settlements with the New York County District Attorney (Manhattan DA), and paid significant forfeitures or fines.

28

Civil Money Penalties and Criminal Enforcement Actions

- How many strikes until you are out?
- Generally, the regulators will cite MRAs in a Supervisory Letter or examination report, followed by a C&D or other public enforcement action before proceeding to assess CMPs either on their own or as part of a global settlement that may include a DPA or forfeiture.
- In egregious situations, however, there may be no prior public enforcement action.
- What is clear is that, as a result of enhanced Congressional scrutiny, the regulators are under pressure to find that BSA deficiencies support a finding of a BSA/AML program violation, to assess CMPs, to bring even more stringent actions against financial institutions, and to bring enforcement actions against bank directors, officers and employees.

29

Recent Criminal Enforcement Actions

- 12/2012 - ***HSBC Holdings plc and HSBC Bank USA, N.A*** - $1.92 billion global settlement with the DOJ, the Manhattan DA, FinCEN, the OCC, the Federal Reserve, and the Treasury Department's Office of Foreign Assets Control for allegedly violating the BSA, the International Emergency Economic Power Act (IEEPA), and the Trading with Enemy Act (TWEA), including for:
  - the failure by HSBC Bank USA to maintain an effective BSA/AML program, conduct Section 312 due diligence on HSBC Group foreign correspondent accounts, and to monitor and report timely suspicious activity, including bulk USD cash deposits and wire transfers with its affiliates, particularly for HSBC Mexico, resulting in the alleged laundering of $881 million in drug and other proceeds; and
  - HSBC Group foreign affiliates' actions in conducting $660 million in OFAC-prohibited transactions on behalf of customers in Cuba, Iran, Libya, Sudan, and Burma, including by omitting customer and country names from USD payment messages and using cover payments to prevent HSBC Bank USA and other U.S. financial institutions from identifying and blocking prohibited payments.

30

Recent Criminal Enforcement Actions

- The HSBC AML program deficiencies included alleged failures to:
  - collect or maintain required CDD or EDD information on HSBC Group Affiliates, which inhibited risk rating and the identification of suspicious activity;
  - monitor adequately wire transfers from customers in “standard” or “medium” risk countries, including from HSBC Mexico which was rated as standard risk;
  - monitor effectively its large wholesale banknote business, including its bulk USD cash transactions with HSBC affiliates, including HSBC Mexico, and clearances of travelers checks;
  - disposition alerts appropriately or file SARs timely, which resulted in significant backlogs;
  - provide adequate staffing and other resources, including automated monitoring systems;
  - provide adequate independent testing; and
  - establish a formal mechanism whereby HSBC Group could share information horizontally among HSBC Group Affiliates.

31

Recent Criminal Enforcement Actions

- 11/2012 - ***MoneyGram International, Inc.*** - $100 million forfeiture and DPA with the DOJ for allegedly aiding and abetting wire fraud in connection with mass marketing and consumer fraud phishing schemes involving corrupt MoneyGram agents that defrauded elderly and other U.S. victims and for failing to maintain an effective AML program, including failing to:
  - implement policies and procedures for filing SARs when victims reported fraud to MoneyGram;
  - conduct adequate due diligence on prospective and existing MoneyGram Agents by verifying that a legitimate business existed;
  - file SARs on agents MoneyGram knew to be involved in fraud and to share information between the fraud and AML functions;
  - implement policies and procedures for terminating agents involved in fraud and money laundering;
  - conduct effective AML audits of its agents and outlets; and
  - sufficiently resource staff and its AML program.

32

Recent Civil Money Penalties

- 1/2013 – ***TCF National Bank*** – $10 million CMP by the OCC for failing to establish and maintain an effective BSA compliance program and file SARs, including failing to:
  - file SARs to report structured cash transactions, wire transfers where the source of funds and purpose was unknown, and out-of-the-ordinary activity; and
  - properly file 13 SARs where transactions indicative of possible terrorist financing were properly identified, investigated, and determined to be suspicious and SARs were filed, but the Bank did not check the "terrorist financing" box or the narrative did not clearly communicate the nature of the activity.
- 11/2012 – ***First Bank of Delaware*** – $15 million CMP by FinCEN and the FDIC for failing to implement an effective BSA/AML compliance program and to detect and report suspicious activity, and a $500,000 civil settlement with the DOJ, related to a scheme by merchants and third party payment processors to defraud consumers that involved debiting consumer accounts using remotely-created checks (RCC) and ACH transactions.
  - The bank's charter and deposit insurance also were revoked in November 2012, and certain of its assets and liabilities were sold.

33

Recent Civil Money Penalties

- First Bank of Delaware's AML program deficiencies included:
  - failing to adequately assess the AML risks associated with third party payment processors, their major ACH merchant clients, and RCC services, and consistently ignoring red flags, including of FTC Act violations, high unauthorized return rates, and higher than anticipated ACH transactions;
  - failing to assess the risks associated with Money Services Business (MSB) customers and conduct site visits of out-of-state, high risk MSBs, including those using remote deposit capture (RDC) services;
  - failing to implement an effective transaction monitoring system for third-party payment processors and high-risk MSBs and that could compare a customer's ongoing activity against its transaction history;
  - failing to designate a BSA compliance officer that could provide effective day-to-day management of the BSA/AML program and escalate BSA problems to the Board and senior management; and
  - failing to conduct adequate independent testing and training for appropriate personnel.

34

Recent Consent Orders

- 1/2013 – ***JPMorgan Chase Bank, N.A., JPMorgan Bank and Trust Company, N.A. and Chase Bank USA N.A. and JPMorgan Chase & Co.*** – Consent Orders with the OCC and the Federal Reserve for BSA deficiencies that resulted in failures to correct previously-reported problems, a BSA/AML program violation, and SAR violations, including:
  - less-than-satisfactory risk assessment processes;
  - inadequate CDD, particularly in the Commercial and Business Unit;
  - systemic weaknesses in transaction monitoring systems, due diligence processes, risk management, and QA programs;
  - a lack of enterprise-wide policies and procedures to ensure that suspicious foreign branch customer activity is communicated effectively to other branches and AML operations and that, on a risk basis, customer transactions at foreign branches can be assessed, aggregated, and monitored;
  - significant shortcomings in SAR decisioning and methods for ensuring that referrals and alerts are properly documented, tracked, and resolved; and
  - inadequate internal controls and ineffective independent testing.

35

Recent Consent Orders

- 4/2012 – ***Citibank, N.A.***– Consent Order with the OCC for failing to implement and adopt an adequate BSA/AML program, develop adequate due diligence on foreign correspondent bank customers, and timely file SARs related to its RDC/international cash letter activity, including:
  - internal control weaknesses, including incomplete identification of high risk clients in many areas, an inability to assess and monitor client relationships on a bank-wide basis, inadequate CDD and periodic reviews, and weaknesses in the scope and documentation of the validation of automated processes;
  - failures to conduct adequate CDD and EDD on foreign correspondent clients, retail banking customers, and international personal banking customers;
  - failing to monitor adequately its foreign correspondent banking RDC/international cash letters and file related SARs timely; and
  - failures by the Bank's independent audit function to identify systemic deficiencies found by the OCC during the examination process.
- 3/2013 – ***Citigroup, Inc.*** – Consent Order with the Federal Reserve calling for holding company measures to address BSA/AML deficiencies and governance.

36

BSA Enforcement Actions

- The penalty and the accompanying publicity is not the end of the pain!
- In many BSA enforcement actions expensive remedial actions are required which can include:
  - Drafting and executing detailed remediation plans.
  - Historical transaction reviews or “look backs” and late filings of SARs for a period of time.
  - Hiring of monitors or independent consultants, approved by the regulator.
  - Periodic detailed reporting to the regulator on progress in implementing the remediation actions.

37

What About Individual Liability and Revocation of Bank Charters?

- There is authority for holding individuals criminally and/or civilly liable for BSA and money laundering violations:
  - Under the BSA, bank directors, officers and employees can be subject to criminal and civil money penalties;
  - The bank regulators can bring enforcement actions against institution-affiliated parties; and
  - Individuals can face criminal liability under the money laundering statutes.
- This authority has been used sparingly (absent overt complicity).
- The death penalty has never been used against a bank.
- In the Wachovia Bank case, there were reports that individual prosecutions were being considered, but they never were brought.
- After the HSBC case, DOJ suggested in public statements that prosecutions against individuals based on BSA compliance failings would be difficult to prove and the domestic or global economic consequences from closing a large bank could be dire.
  - This has been referred to “as too big to jail.”

38

Post HSBC Congressional Hue and Cry for More Draconian Action

- December 12, 2012 – Former Chairman of the House Financial Services Committee, Barney Frank, sent a letter to the Attorney General urging criminal prosecutions of banks and individuals for financial crimes.
- March 2013 – Senate Judiciary and Banking Committee Hearings – The DOJ evoked the wrath of several Senators, notably Elizabeth Warren (D-MA), who led the charge in questioning the Attorney General, the Treasury Department, the Federal Reserve, and the OCC. She said:

> "If you are caught with an ounce of cocaine, the chances are good you are going to go to jail . . . . But evidently, if you launder nearly a billion dollars from drug cartels and violate our international sanctions, your company pays a fine and you go home and sleep in your own bed at night . . . ."

39

The Dilemma for Bank Compliance and Risk Officers, Bank Lawyers, and Others

- In response, Treasury has indicated that, in appropriate cases, it will seek to use its authority under the BSA (and OFAC) to bring more enforcement actions against individual financial institution employees.
- The OCC is exploring the possibility of regulatory changes that would enhance its ability to take removal and prohibition actions against bank directors, officers, and employees that engage in violations of the BSA.
- The prospect of individual enforcement actions or prosecution presents a dilemma for bank employees responsible for BSA compliance.
  - What should a bank employee do if the bank refuses to address the risks or ignore possible money laundering activity?
  - Should the employee work to try to improve the situation from within? Resign? Become a whistleblower?
  - What effect will individual enforcement actions/prosecutions have on attracting talented compliance professionals?

40

Common Problems and Issues That Lead to BSA Meltdowns

- Breakdowns in communication between a bank and its regulators.
- Failures to correct deficiencies identified in previous exams and make BSA compliance a high priority.
- Lack of a strong tone from the top and compliance culture throughout the organization.
- Weak compliance structure – inadequate authority and independence from the business lines, inadequate or unqualified staff.
- Weak audit function – poor coverage and planning, inadequate compliance testing, poorly trained auditors, no audits of systems that support the AML functions.
- Compliance done on the cheap – staff, technology, outside consultants.
- Antiquated systems – lack of technology support and MIS reporting.
- Inadequate risk assessments and CDD– failures to identify high risk products and clients and to treat affiliates like other customers.
- Ineffective suspicious activity monitoring systems.
- SAR backlogs – Failures to investigate alerts and file accurate SARs timely.
- No subpoena reviews.
- Poor training.

41

What Can Banks Do to Steer Clear of Enforcement Actions?

- Catch problems before your regulators, be responsive to their concerns. and correct deficiencies identified in examinations and internal audits.
- Establish a strong AML governance and oversight structure and compliance culture, and make compliance a top priority.
- Integrate compliance incentives and discipline into the AML program.
- Provide your AML officer with adequate authority and independence from the business lines, and staff the compliance function with qualified and sufficient staff.
- Foster good communication between Compliance and the business lines and share information across the organization.
- Escalate significant issues to senior management and the Board.
- Treat your affiliates no differently than other customers.
- Conduct periodic risk assessments, including of new products and acquisitions; do not introduce new products without proper BSA/AML controls; and refresh your AML program.

42

What Can Banks Do to Steer Clear of Enforcement Actions?

- Ensure that CDD and EDD information is obtained and updated periodically and in response to triggering events.
- Invest in the right type of technology to monitor transactions for suspicious activity, and customize, fine-tune, and validate parameters.
- Invest in case management and MIS systems and identify backlogs.
- Review criminal subpoenas.
- Investigate Section 314(a) matches and review responses to Section 314(b) sharing requests.
- Develop procedures for reviewing multiple SARs and terminating customer relationships.
- Ensure that the auditors are well-trained and that independent testing is sufficiently broad and includes testing to ensure that previous examination, audit and compliance issues have been corrected.
- Keep abreast of enforcement actions – see where others have fallen short and make sure that you are not vulnerable to the same weaknesses.

43