

AML ENFORCEMENT ACTIONS:

BY JOHN J. BYRNE, CAMS, AND MICHAEL D. KELSEY

From the government's perspective, I think we need to be very careful to properly communicate our message when we take enforcement actions. The message is not only to the targeted institution, but to the industry as a whole and we have to remember that. I think our enforcement actions should be public, and these actions should provide a written road map from which other institutions can learn. We cannot afford to have the tactical overtake the strategic. From the industry, it seems to me we need two things: 1) we need you to not overreact to our enforcement actions, but to read, study, and learn from the road maps we provide you when we take such actions. If our road maps are ambiguous, or if they leave questions, then we need you to ask those questions—I'll promise we'll get you the answers; and, 2) we need your continued commitment to institute programs, policies, procedures and systems to protect your institution and the U.S. financial system from the abuses posed by criminals and terrorists.

—William J. Fox, former FinCEN director at the 2004 ABA/ABA Money Laundering Enforcement Seminar



AS WE PROGRESS

through 2006 and continue to face myriad challenges in the critical area of anti-money laundering (AML) compliance, what can we glean from the spate of enforcement actions issued in the past year? William J. Fox, Financial Crimes Enforcement Network's (FinCEN's) former director, has made clear that one of his agency's

goals is to use enforcement actions

as a training tool for the financial sector. In equally

forceful terms, other agency leaders have recommended caution, lest a bank read too much into a particular order, as the orders are clearly fact-based.

We believe that the answer lies somewhere in between—understanding the general reasons for an institution's penalty but recognizing that the order is not a template for action.

The dilemma for the industry, of course, is that we ignore enforcement “**themes**” at our peril. Vendors, consultants, auditors, and even examiners certainly alter their AML oversight based on these actions. At the end of the day, what can we learn?

This article provides brief summaries of the major actions that suggest themes (in bold) of changes in AML policies for compliance officers.

What Can We Learn?

BANCO DE CHILE October 12, 2005

AFTER FEDERAL RESERVE BOARD (FRB) and Office of the Comptroller of the Currency (OCC) consent orders against the Miami and New York branches in February 2005, a separate FinCEN investigation resulted in a \$3 million civil money penalty against Banco de Chile for violations of the Bank Secrecy Act (BSA).

In Banco de Chile-New York, FinCEN found the following:

- The bank's customer identification program (CIP) was deficient in that it did not require a customer's identification number, did not include procedures for providing customers with notice of the requirements of the regulation, did not provide for independent testing, did not describe when a suspicious activity report (SAR) should be filed, and did not describe parameters for account closure in the absence of verification of a customer's identity.

- Significant deficiencies were noted in the identification and monitoring of politically exposed persons (PEPs), customer account due diligence procedures, monitoring for potential suspicious activity, structure and staffing of the compliance function and the independent audit function.

In Banco de Chile-Miami, FinCEN found the following:

- Even though the definition of PEPs, as provided in Banco de Chile-Miami's AML program, was in line with regulatory guidance from the Federal Reserve, in practice the definition was too narrowly applied. As a result of these deficiencies, suspicious activity occurring in a PEP's account went unreported and was deemed not timely.

- The Miami branch's **log of investigations did not effectively track open investigations.**

The scope of the audits did not adequately test new account reviews, compliance with CIP requirements, wire transfer and cash activity, account monitoring, and reviews of existing accounts (particularly for high-risk accounts) for adequate due diligence. For both branches, FinCEN found the following: Due to failures in their AML compliance to failures in their AML compliance programs, neither branch identified, reviewed, or evaluated numerous large dollar value transactions by, for, or on behalf of a prominent PEP and a family member and associate of the prominent PEP. As a result, both Banco de Chile-New York and Banco de Chile-Miami were deemed to have failed to timely report suspicious activity involving millions of dollars.

DEUTSCHE BANK TRUST COMPANY October 14, 2005

DEUTSCHE BANK ENTERED INTO a written agreement with the Federal Reserve Bank of New York and the New York State Banking Department that "addresses Bank Secrecy Act and anti-money laundering compliance at Deutsche Bank Trust Company Americas, including policies and practices relating to the provision of correspondent banking services."

The major focus of the agreement related to the bank's "significant correspondent banking services to both U.S. and non-U.S. banks," as well as its conducting a "high volume of U.S. dollar funds transfer clearing for its respondent banks." The government announced that the bank agreed to take specified steps to address deficiencies relating to AML compliance.

The following were among those steps:

- Provide for **thorough assessment of legal and reputational risks associated with correspondent banking and funds transfer clearing activities**, and conduct a regular review of risk tolerance by appropriate members of senior management of the bank.

- For correspondent accounts established, maintained,

administered, or managed in the United States for a foreign financial institution, **establish procedures that comport with industry sound practices set forth in available public guidance [(e.g. the New York Clearing House Association LLCs "Guidance for Counter Money Laundering Policies and Procedures in Correspondent Banking" (March 2002) and the Basel Committee on Banking Supervision's "Customer Due Diligence for Banks" (October 2001)].**

- Implement procedures for reviewing potentially suspicious activity, such as patterns of large U.S. dollar transactions effected through high-risk jurisdictions, and high-dollar transfers where transaction volumes or amounts do not have valid business purposes based on available information regarding the parties (including shell corporations), or where such information is unavailable or apparently inaccurate.

- Maintain sufficient documentation with respect to the bank's investigation and analysis of suspicious activity, including the resolution and escalation of concerns.

- Implement procedures for determining when the closing of an account is warranted, affecting such closures in a timely manner and documenting such determinations.

Quantity of Risk

Conclusion: The quantity of risk is (low, moderate, high).

Objective: Determine the level of compliance with BSA, AML, and OFAC requirements.

Reporting, Record Keep

KEY BANK, N.A. October 17, 2005

BASED ON DEFICIENCIES FOUND in the bank, the order requires Key Bank to do the following:

- Institute a process to assess, identify, and assign risk to customers, products, services, and geographies that identifies and addresses gaps in management of BSA risk; this risk assessment should be consistent with the “Quantity of Risk Matrix” found in the *Bank Secrecy Act Anti-Money Laundering Examination Manual*.

- Implement suspicious activity monitoring controls for all appropriate lines of business (LOB) and functional areas that are commensurate with the level of risk identified in each LOB to ensure suspicious activity monitoring in all LOBs.

- Establish procedures that indicate the tools or processes to be used for all LOBs with BSA risk for identifying and monitoring high-risk transactions.

- Establish well-defined procedures for investigating and resolving the bank’s response to transactions it identifies as unusual or suspicious.

- Ensure reasonable procedures that comply with 31 C.F.R. Section 103.121 for the opening of new accounts; this information should be readily retrievable for independent review or upon the request of regulators.

- Create policies, operating procedures, due diligence programs, and quality control systems that ensure **at least an annual risk-focused assessment of the bank’s customer base**.

- Implement investigation case file standards **that are consistent** with the SAR decision-making process section of the *Bank Secrecy Act Anti-Money Laundering Examination Manual*.

- Develop a method for **evaluating new products and services** that ensures that the procedures governing new products and services are consistent with the bank’s program for compliance with the BSA.

In addition, the bank’s board must develop, implement, and ensure bank maintenance of an accurate system, manual or automated, **to produce periodic reports for all bank LOBs designed to identify unusual or suspicious activity**, including patterns of activity, and to monitor and evaluate unusual or suspicious activity.

The bank is also required to upgrade the function of the BSA officer by requiring that the BSA officer, in conjunction with the internal auditors, “ensure the adequacy of the identification of BSA deficiencies, the adequacy of BSA-related internal controls throughout the bank, the adequacy of testing risks and BSA-related internal controls, and the timeliness of corrective action.”

Finally, the bank must ensure that employees in each LOB with BSA risk obligations **receive additional training concerning suspicious activity** in any other BSA risks specific to that LOB.

ABN AMRO December 19, 2005

THE FEDERAL RESERVE BOARD, the New York State Banking Department, the Illinois Department of Financial and Professional Regulation, FinCEN, and the Treasury’s Office of Foreign Assets Control (OFAC) released a consent cease and desist order and civil penalties against ABN AMRO and its branches in New York and Chicago for, among other things, systemic defects in the bank’s internal controls.

According to the press release,

The agencies have assessed penalties based on findings of unsafe and unsound practices; on findings of systemic defects in ABN AMRO’s internal controls to ensure compliance with U.S. anti-money laundering laws and regulations, which resulted in failures to identify, analyze, and report suspicious activity; and on findings that ABN AMRO participated in transactions that violated U.S. sanctions laws. ABN AMRO is also required to take ongoing measures to ensure compliance with U.S. sanctions laws.

In FinCEN’s civil money penalty (CMP) assessment, the Treasury bureau found the following:

- The North American Regional Clearing Center, a unit within the New York branch of ABN AMRO, operated as a

clearing institution for funds transfers in U.S. dollars. The center processed about 30,000 funds transfers per day, including about 400 unaffiliated institutions. FinCEN concluded that the bank failed to apply “an adequate system of internal controls reasonably designed to assure compliance with the Bank Secrecy Act.” The New York branch also **lacked adequate staff** to coordinate and monitor BSA compliance.

- The New York branch staff did not receive adequate AML training.

- FinCEN found that because the bank did not risk-rate the unaffiliated financial institutions for which it provided funds-transfer clearing services, there were deficiencies in its internal controls system due to the volume of funds transfers, which FinCEN believed “posed a substantial risk of money laundering.” FinCEN criticized the bank for failure to assess the risk of money laundering that each unaffiliated institution posed.

- The New York branch failed to adequately monitor funds transfers for suspicious activity and lacked sufficient automated monitoring. To the extent it utilized automated monitoring, the bank failed to investigate numerous alerts generated by the system.

■ In the area of suspicious activity, the bank had extensive violations of the suspicious activity reporting requirements, **failing to file timely SARs or filing incomplete or inaccurate SARs.**

In FRB's and OFAC's CMP assessment, the agencies found the following:

■ The bank lacked adequate risk management and legal review policies, which enabled its overseas branches to circumvent OFAC procedures with certain funds transfers, check clearing operations, and letter of credit transactions.

■ The bank **did not follow up on findings from**

internal audits, failed to produce negative audit findings to U.S. regulatory supervisors, and overstated the extent of its due diligence to those same regulators and its internal auditors.

■ OFAC penalties were for transactions, direct or indirect, to Iran and Libya.

The bank has agreed to a management plan for internal controls, OFAC compliance, and the development of processes to ensure that any business line includes full due diligence (appropriate oversight, controls, compliance, and risk monitoring and reporting).

OPPENHEIMER BROKER-DEALER December 29, 2005

ON DECEMBER 30, the New York Stock Exchange (NYSE) and FinCEN announced the last civil money penalty for AML-related deficiencies in 2005. The \$2.8 million CMP (2005-4) was issued against Oppenheimer & Company, Inc., a securities broker-dealer located in New York City with foreign branches as well as a Florida branch office and many others throughout the United States. Oppenheimer was cited for deficiencies in its BSA program requirements, including failures to "properly identify and report" suspicious transactions.

According to the press release, William Fox pointed out, "Today's action reinforces our message to all financial institutions, whether a bank or securities-broker dealer, about the importance of having effective anti-money laundering programs and controls in place to manage the risks of money laundering."

In FinCEN's CMP assessment, the Treasury bureau found the following:

■ Oppenheimer had been notified by the NYSE and the Securities and Exchange Commission (SEC) of procedural deficiencies in 2001, 2003, and 2004. These problems affected the institution's ability to file timely and complete SARs.

■ FinCEN found deficiencies in the system of internal

controls with respect to "journal transactions and wire transfers," which involved "unrelated and related customer accounts." The institution lacked an adequate system to review these transactions, which "lacked related securities transactions and appeared to lack economic benefit."

■ Wire activity was manually reviewed by one compliance employee and "none of the reports used to facilitate suspicious activity reporting compliance aggregated incoming or outgoing wire transfers by customer, account, branch office, or destination." As a result, FinCEN concluded that **these reports "did not capture a true picture of a customer's total money movements."**

■ Oppenheimer lacked an adequate system for independent testing of BSA compliance. For example, the institution's internal audit did not include higher-risk activities between foreign and domestic branches. FinCEN also criticized the fact that the internal audit department played a "supervisory role in finalizing any decision regarding the reporting of suspicious activity." The Treasury bureau looked at that system and concluded that the overlap of AML compliance and auditing responsibilities created a potential conflict of interest, compromising "the independence of Oppenheimer's anti-money laundering testing."

PINEBANK, NATIONAL ASSOCIATION February 15, 2006

ON FEBRUARY 15, the Office of the Comptroller of the Currency (OCC) announced two consent orders (2006-1 and 2006-2) over Pinebank, National Association (Miami) and the Summit National Bank (Atlanta) covering AML deficiencies.

The bank agreed to address a number of problems. In the area of AML program improvement, the OCC directed Pinebank to ensure that it had a risk-based program that covers "all lines of business, including domestic and international operations." In addition, Pinebank must create "adequate controls and procedures to perform transaction

testing on all accounts of bank affiliates, and affiliates of bank shareholders, to detect suspicious activity." The order also emphasizes the following:

■ stringent and effective due diligence over foreign correspondent bank accounts sufficient to prevent violations of the USA PATRIOT Act and the BSA

■ adequate controls and transactional testing procedures over correspondent bank accounts to ensure that

- ▶ account profiles include documentation on the purpose of the account, how it is to be used (including third-party transactions), and the funding base

While we strongly caution that you do not treat the conclusions in orders as regulations— We know the examiners will be reading the same orders—

- ▶ transaction and volume limits are established and the bank monitors accounts for any deviation from those limits
- ▶ the nature and purpose of transactions in the accounts conform to account profiles and expectations
- ▶ transactions outside profile limits are documented and investigated, and appropriate action is taken by the bank

The bank must also develop a **“comprehensive training program for all appropriate personnel to demonstrate sufficient knowledge of the nature and volume of third-party transactions processed through correspondent bank accounts, and how to monitor those accounts for suspicious activity using automated reports and other resources.”**

In the area of audits, the Pinebank board agreed to implement a comprehensive audit program that on an annual basis uses a risk-based approach to require, among other things

- sufficient coverage to evaluate the adequacy of internal controls designed to ensure compliance with the provisions of the BSA
- transactional testing of 100 percent of high-risk ac-

counts that are internally rated “3” with a smaller random sample covering low- and medium-risk accounts that are internally rated “1” to “2,” to include verification and testing of all account activity over a minimum period of at least 90 days

- transactional testing of affiliate accounts over a minimum period of 90 days
- review of a minimum of 10 percent of accounts internally rated medium to low to determine whether the ratings are appropriate
- review of 100 percent of private investment companies/bearer share accounts
- a high level of transactional testing for correspondent banks, PEPs, and money service businesses (MSBs)
- evaluation of the bank’s due diligence efforts and monitoring processes for foreign correspondent bank accounts
- validation of know-your-customer profiles to determine whether profiles were established consistent with bank policy, that profiles were reviewed and approved by bank management, and that the bank’s compliance function effectively ensures that accounts comply with bank policy and regulations

THE SUMMIT NATIONAL BANK January 2006

SUMMIT NATIONAL BANK agreed to correct deficiencies in its audit function as well as with CIP and AML training. The detail of the order is striking. The OCC went to great lengths to outline adjustments that needed to be made with internal controls, stressing that the AML program needed a series of changes, including the following:

- an ongoing and comprehensive process to assess, identify, and assign risk levels to customers, products, services, and geographies, consistent with the “Quantity of Risk Matrix” included as Appendix J to the *Bank Secrecy Act Anti-Money Laundering Examination Manual*, and to evaluate the quality of BSA risk management in each line of business and functional area
- implementation of suspicious activity monitoring controls for all LOBs, including controls in each LOB that are commensurate with the level of risk identified in that LOB to ensure suspicious activity monitoring in all LOBs
- a governance structure with clear lines of responsibility beginning with senior management and including each LOB, in which accountability for BSA compliance is clearly communicated and enforced
- enhanced policies and procedures for recording, maintaining, and recalling information about transactions that pose greater than normal risk for BSA compliance
- well-defined policies and procedures for investigating and resolving the bank’s response to transactions that the bank identifies as unusual or suspicious

■ comprehensive procedures to identify and report to appropriate management personnel

- ▶ frequent or large-volume cash deposits or wire transfers or book entry transfers to or from offshore or domestic entities or individuals
- ▶ wire transfers or book entry transfers that are deposited into several accounts
- ▶ receipt and disbursement of wire transfers or book entry transfers without an apparent bona fide business reason
- ▶ receipt and disbursement of wire transfers or book entry transfers that are suspicious or inconsistent with the customers’ business
- ▶ receipt and disbursement of currency or monetary instruments that are suspicious or inconsistent with the customers’ business
- ▶ accounts opened in the name of or for the benefit of a “financial institution” as defined in 31 C.F.R. Section 103.11(n) or “foreign bank,” as defined in 31 C.F.R. Section 103.11(o)

Another area of focus was risk assessment with new products. The order requires “a method for introducing new products and services that ensures that the policies and procedures governing new products and services are consistent with the bank’s program for compliance with the Bank Secrecy Act.”

Finally, the bank is required to “develop, implement,

or rules for all institutions, there is merit to recognizing common areas of deficiency.—so at a minimum, so should compliance officers.

document in writing, and thereafter ensure bank **maintenance of an integrated, accurate system for all Bank areas to produce periodic reports designed to identify unusual or suspicious activity, including patterns of activity, to monitor and evaluate unusual or suspicious activity, and to maintain accurate information needed to produce these reports.**” Specifically, the order mandates the following:

■ The bank’s systems shall be able to link related accounts, countries of origin, and location of the customers’ businesses and residences to evaluate patterns of activity.

■ The bank shall maintain, either manually or through the bank’s electronic information systems, a list of all accounts associated with a relationship, a country or a politically exposed person.

■ The periodic reports shall cover one day, a number of days, and monthly reports and shall segregate transactions that pose a greater-than-normal risk for compliance with the Bank Secrecy Act.

■ The periodic reports shall include reports on all accounts posing greater than normal risk for compliance with the Bank Secrecy Act that are newly established, renewed, or

modified, including the following information:

- ▶ the name of the customer
 - ▶ the officers, directors and major shareholders of any corporate customer and the partners of any partnership customer
 - ▶ any other accounts maintained by the customer and, as applicable, its officers, directors, major shareholders, or partners
 - ▶ a detailed analysis of the due diligence performed on the customer and, as applicable, its officers, directors, major shareholders, or partners
 - ▶ any related accounts of the customer at the bank
 - ▶ any action the bank has taken on the account
 - ▶ the purpose and balance of the account
 - ▶ any unusual activity for each account;
- The periodic reports shall include reports on any type of subpoena received by the bank and on any law enforcement inquiry directed to the bank, any action taken by the bank on the affected account.
- The periodic reports shall include reports deemed necessary or appropriate by the BSA officer or the bank.

Conclusion

While the industry recognizes that all AML/BSA enforcement actions are fact-based, there are indeed lessons to be learned from any penalty assessed for deficiencies in these programs. While we strongly caution that you do not treat the conclusions in orders as regulations or rules for all institutions, there is merit to recognizing common areas of

deficiency. We know the examiners will be reading the same orders—so at a minimum, so should compliance officers.

Our challenge is to always improve our systems without making changes that are unnecessary or at least unwarranted by the facts. Working with our government partners to separate the wheat from the chaff is the best method of accomplishing this goal. BC

ABOUT THE AUTHORS

After 22 years with the American Bankers Association, **John J. Byrne, CAMS**, joined Bank of America as senior vice president for AML strategies. In this role, he is responsible for working with federal and state regulatory agencies, law enforcement, and industry organizations on AML-related issues. Prior to joining Bank of America, John was most recently director of the ABA Center for Regulatory Compliance.

Byrne, who has represented the ABA before Congress, state legislatures, and various regulatory agencies as well as in the electronic and print media, has also been a member of the Treasury Department’s Bank Secrecy Act Advisory Group (BSAAG) since its inception and co-chairs the American

Bar Association/American Bankers Association Annual Money Laundering Enforcement Seminar. He also co-chairs the BSAAG examination subcommittee. Byrne has written extensively on money laundering and privacy issues and is a frequent contributor and adviser to Money Laundering Alert, Bankers Hotline, ABA Bank Compliance magazine, and other banking publications.

He was also the first private sector recipient of the “Director’s Medal for Exceptional Service” from the Treasury Department’s Financial Crimes Enforcement Network (FinCEN). He received his undergraduate degree from Marquette University in Milwaukee, Wis., and his J.D. from George Mason University in Arlington, Va. He is a member of the District of Columbia and Pennsylvania Bars. Reach him by telephone

at (202) 351-0118 or via e-mail at john.j.byrne@bankofamerica.com.

Michael D. Kelsey is director of anti-money laundering risk management for PNC Financial Services Corp. He began his career with PNC in 1985 as securities counsel at Bank of Delaware, which was acquired by PNC in 1988. He has held a variety of positions in PNC’s Legal and Compliance departments. Kelsey graduated from Widener University Schools of Law in 1983, has taught Banking Law at Widener as a member of the adjunct faculty, and writes and speaks frequently on compliance and AML risk issues. He is also chair of the American Bankers Association Compliance Executive Committee. He lives with his family in Wilmington, Delaware. Reach him by telephone at (302) 429-1775 or via e-mail at michael.kelsey@pnc.com.