2005

Recent Developments in Bank Secrecy Act Enforcement

Robert S. Pasley

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi
Part of the Banking and Finance Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncbi/vol9/iss1/5

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
RECENT DEVELOPMENTS IN BANK SECRECY ACT ENFORCEMENT

ROBERT S. PASLEY

I. INTRODUCTION

For over thirty years, the Bank Secrecy Act of 1970 (BSA) has required financial institutions to maintain records and to make certain reports to federal regulators to assist in various criminal, tax or regulatory proceedings. In this fashion, financial institutions play an integral role in detecting money laundering of illicit funds. After the terrorist attacks of September 11, 2001, new laws and regulations were issued to address money-laundering and terrorist financing, thus, increasing the role of financial institutions in preventing such activity. As set forth in the recent "Statement of Offense" involving the plea agreement by Riggs Bank N.A., "[f]rom the U.S. government’s perspective, the BSA regulatory regime constitutes law enforcement’s first defense against the misuse of the U.S. financial system by money launderers and terrorist financiers."2

This article explores the increasing perils to financial institutions whose anti-money laundering efforts and programs are deficient. In Part II, the article provides a brief overview of the statutory and regulatory regime governing money laundering. In Part III, the article examines two actions brought against banks that resulted in substantial administrative civil money penalties, and also, in one case, resulted in a criminal fine. In Part IV, the article examines the cases involving four other banks that have faced criminal actions based on the failure to file required reports under the BSA. The actions that

---

1. Robert S. Pasley is an Assistant Director of the Enforcement & Compliance Division of the Office of the Comptroller of the Currency. The views expressed in this article are Mr. Pasley’s and do not necessarily reflect the views of the Office of the Comptroller of the Currency.

led to these charges are explored in detail, as well as some of the controversy involving these cases. In Part V, the article concludes that the cases illustrate the necessity for financial institutions to have a strong BSA compliance programs in place, and provides specific suggestions for how to design and implement such programs.

II. A BRIEF BACKGROUND OF ANTI-MONEY LAUNDERING

Banks are required, pursuant to the BSA, to file a Suspicious Activity Report ("SAR") whenever they detect possible violations of criminal law or suspicious activity, as set forth below. This requirement replaced the criminal referral process and became effective on April 1, 1996.3

In summary, a bank is required to report a transaction conducted, or attempted to be conducted, through the bank (subject to certain monetary thresholds) if the bank knows, suspects, or has reason to suspect that:

a. the bank was an actual or potential victim of a criminal violation;

b. the transaction involved funds derived from illegal activities or was intended or was conducted in order to hide or disguise funds or assets derived from illegal activities as part of a plan to violate or evade any federal law or regulations or to avoid any transaction reporting requirement under federal law;

c. the transaction was designed to evade any regulations promulgated under the BSA; or

d. the transaction had no business or apparent lawful purpose or was not the sort in which the particular customer would normally be expected to engage and the bank knows of no reasonable explanation for the transaction after examining

the available facts, including the background and possible purpose of the transaction.

In addition to the requirement to file SARs, banks are required, pursuant to the BSA, to file a Currency Transaction Report ("CTR") for each non-exempt deposit, withdrawal, exchange of currency, or other payment or transfer by, through, or to the bank that involves currency of more than $10,000. Banks are also required to verify and record on a CTR the true name and address of the individual presenting the transaction, as well as the true nature of the entity or person on whose behalf the transaction is effected.

III. CIVIL ENFORCEMENT ACTIONS AND CIVIL MONEY PENALTIES UNDER THE BSA

The bank regulatory agencies and FinCEN may seek civil money penalties for violations of the BSA. Two cases, one involving UBS and one involving Riggs Bank, resulted in record civil money penalties of $100 million and a $25 million, respectively.

A. UBS Case

In April 2003, United States armed forces seized the palace of Saddam Hussein in Baghdad. This was, of course, an important military and psychological development in the war in Iraq. It also led, however, to a strange development in the fight against money laundering. Unexpectedly, the armed forces found $650 million in United States currency in neat stacks of $100 bills placed in 164 metal boxes, all riveted shut. Most of the money was new, sequentially numbered and still in its shrink-wrapped containers. The initial question, of course, was: how did the money get there?

Within days of the currency being discovered, the New York Federal Reserve Bank ("NY Fed") had obtained a sample of serial

---

numbers from the money and had traced the money to shipments of U.S. banknotes to three banks: HSBC in London, Bank of America in Zurich and UBS in Zurich. The shipments were made in conjunction with a program entitled “Extended Custodial Inventory,” or “ECI.”

This program began in 1996 and is managed by the Federal Reserve in order to facilitate, monitor and control the international distribution of U.S. banknotes. This is a particularly important function in light of the fact that almost two-thirds of the dollar value of all U.S. banknotes is in circulation overseas. As a result, only five specifically selected banks are permitted to participate in the program.

During the course of investigating this matter, the NY Fed received a report from UBS in June 2003, indicating that the bank had made eight shipments of U.S. banknotes to Iran, a country (like Iraq) that was on the Office of Foreign Assets Control (OFAC) list of sanctioned countries. UBS claimed that the eight shipments to Iran and the bank’s failure to report the shipments on the bank’s monthly reports to the Fed “were the result of an innocent mistake.” In order to explore this development further, the NY Fed had UBS direct its outside auditor, Ernst and Young, to perform a more thorough review. E&Y determined that, in fact, UBS had also engaged in banknote transactions with Cuba, another OFAC sanctioned country, and that UBS had similarly failed to report this to the NY Fed.

In October and November 2003, UBS finally acknowledged that it had also engaged in prohibited banknote transactions with Libya and the former country of Yugoslavia (currently the Republics of Serbia and

---

8. Id. at 1.
9. Id. at 2.
10. Id.
11. Id. at 3.
12. Baxter, supra note 7, at 6-7. Engaging in transactions with OFAC listed countries was specifically prohibited by the ECI Agreement the Fed had with each of the custodial banks participating in the program. Id.
13. Id. at 7.
14. Id. at 8.
15. Id.
Montenegro). In other words, UBS had engaged in prohibited transactions with four OFAC listed countries and had not disclosed any of the transactions to the Federal Reserve.

The NY Fed ultimately determined that, far from these transactions being "an innocent mistake," UBS had consistently engaged in these transactions from the inception of the ECI program, had taken affirmative actions to conceal the transactions from the NY Fed, had falsified its monthly reports to the NY Fed and had even continued the concealment and deception long after the commencement of the investigation into the discovery of the U.S. banknotes in the palace of Saddam Hussein. The deception had persisted over the course of eight years.

As a result of UBS's conduct, the Federal Reserve, in October 2003, terminated its ECI agreement with UBS. This alone was a severe rebuke for UBS. On May 10, 2004, however, the Federal Reserve followed up with a record breaking civil money penalty of $100 million against UBS. The Federal Reserve justified the amount of this penalty, in part, by pointing to the size of UBS ($1 trillion), its aggregate net profits of $87 million for all banknote transactions for all currencies with all countries and its net profit of $5 million with the four countries noted above. The Federal Reserve also analogized to the $100 million civil money penalty it had assessed against Credit Lyonnais for engaging in a "similar pattern of deliberate and repeated false statements to the Federal Reserve" in connection with that bank's undisclosed acquisition of another company. Not reflected in the public statements or documents, but potentially a contributing factor in arriving at the large dollar amount, was the fact that a brokerage subsidiary of UBS had been sanctioned by the Financial Services Authority (FSA) in the United Kingdom in 2001 with the then second

16. Id. at 8-9.
18. Id.
19. Id. at 10.
20. Id. at 11.
22. Baxter, supra note 7, at 11-12.
23. Id. at 12.
largest fine (350 pounds – or approximately $510,000 at the time) ever imposed by the FSA for having poor anti-money laundering controls.\textsuperscript{24} While this sanction was for conduct in 1998 and 1999, approximately 11 months prior to UBS acquiring the subsidiary, the charges themselves were brought nine months after UBS’s acquisition of the subsidiary.\textsuperscript{25}

The Federal Reserve’s civil money penalty document against UBS indicates that the $100 million penalty was for: (1) engaging in “U.S. dollar banknote transactions through the Zurich ECI with counterparties in jurisdictions subject to sanctions by the Office of Foreign Assets Control of the U.S. Department of the Treasury, specifically, Cuba, Libya, Iran, and Yugoslavia;” and (2) engaging “in intentional acts aimed at concealing those banknote transactions from the Reserve Bank, including, but not limited to, the falsification of monthly reports submitted by UBS to the Reserve Bank.”\textsuperscript{26} However, in his testimony ten days after the assessment was levied, Mr. Baxter indicated that the remedy for the actual breach of the ECI Agreement was the termination of the ECI Agreement with UBS.\textsuperscript{27} He indicated that the $100 million penalty was solely to punish UBS for its deception.\textsuperscript{28}

One obvious moral to take away from this case is that one should not lie to or try to deceive one’s regulator. But that is overly simplistic. While this case was very unusual, involving a huge amount of money, a highly visible and sensitive international matter, U.S. banknote transactions in foreign countries handled by only five large banks, and a program that “is critical to ensuring the quality of U.S. currency abroad,”\textsuperscript{29} it lends itself to some fundamental principles applicable to all banks.

First, UBS’s failures indicate a lack of internal controls that


\textsuperscript{25} Treanor, supra note 24.

\textsuperscript{26} Federal Reserve UBS Assessment, supra note 21, at 1-2.

\textsuperscript{27} Baxter, supra note 7, at 11.

\textsuperscript{28} Id.

\textsuperscript{29} Id. at 4.
should have been in place to prevent the illegal transactions. A properly designed set of controls should have been able to preclude the bank from engaging in multiple transactions with Iran and three other OFAC sanctioned countries. Second, the case reflects a lack of a proper audit that should have discovered, much earlier than it did, the fact that the bank’s monthly reports to the Federal Reserve were false. Clearly, the bank had internal reports that reflected the eight shipments to Iran given the fact that these reports were belatedly disclosed to the NY Fed. In addition, there were reports which enabled E&Y to determine that the bank had engaged in additional banknote transactions with Cuba. An adequate audit function should have been in place to review and to analyze these reports and to bring them to the attention of the board of directors of the bank. Third, UBS’s failures underscore a lack of training. In order for the bank to have engaged in these transactions over an eight-year period, a number of employees had to have been involved. For this to have persisted for as long as it did, there had to have been a carelessness, at best, in training employees to ensure that they understood the nature of the restrictions in the ECI program and the importance of adhering to them.

Internal controls, audit and training are, of course, three of the four fundamental requirements for a BSA program.30 UBS, it appears, failed to have any of these in place. What is significant in this regard is the Federal Reserve’s decision to allow the other two banks which were linked to the U.S. banknotes found in Iraq – HSBC and Bank of America – to continue with the ECI program because, according to Mr. Baxter, the Federal Reserve was sufficiently comfortable with those banks’ procedures for compliance with OFAC regulations and anti-money laundering statutes and regulations.31

In order for any bank to have the proper policies and procedures in place, it must have proper direction from senior management and the board of directors. Conversely, even if a bank has all the right policies and procedures in theory, if the culture instilled in the bank by the board and senior management is not sufficiently strong and supportive of a comprehensive compliance regime, those policies and procedures will ultimately have little effect. The result will likely be adverse not only

for the bank, but also for the board. Very simply, if the direction and commitment to compliance is not taken seriously, emphasized and communicated from the board and senior management, it will not be adequately received, understood and adhered to throughout the bank.

B. Riggs Case

Three days after the Federal Reserve issued its $100 million civil money penalty against UBS, the Office of the Comptroller of the Currency, together with the Financial Crimes Enforcement Network (FinCEN), assessed Riggs Bank NA, McLean, Virginia, a civil money penalty of $25 million.32

According to the OCC’s Press Release, “the bank had failed to implement an effective anti-money laundering program. As a result, it did not detect or investigate suspicious transactions and had not filed Suspicious Activity Reports as required under the law.”33 As set forth more completely in its “Consent Order of Civil Money Penalty” against Riggs, the OCC found that the bank had failed to comply with all four elements required of a BSA compliance program.34 FinCEN, in its “Assessment of Civil Money Penalty,” echoed the OCC’s findings:

FinCEN has determined that Riggs willfully violated the suspicious activity and currency transaction reporting requirements of the BSA and its implementing regulations, and that Riggs has willfully violated the anti-money laundering program . . . requirement of the BSA and its implementing regulations. The violations Riggs engaged in were systemic – Riggs was deficient in designing a program tailored to the risks of its

---


33. OCC Riggs Press Release, supra note 32.

business that would ensure appropriate reporting, implementing the procedures it did have, and responding to classic "red flags" of suspicious conduct.\textsuperscript{35}

With regard to internal controls – the first required component of a BSA program – the OCC found that:

The Bank’s internal controls were . . . seriously deficient. The Bank’s system of internal controls did not effectively identify or address the BSA-related risks that existed in various divisions of the Bank or that related to customers, products, services, or accounts that should have been viewed as high risk. Moreover, the Bank’s Anti-Money Laundering and Enhanced Due Diligence program and Customer Identification Program pertaining to areas deemed to be high-risk were not adequately implemented.\textsuperscript{36}

Similarly, FinCEN found that:

Riggs’ internal controls were not designed to take into account the exposure posed by the customers, products, services, and accounts from high-risk international geographic locations that are commonly viewed as high-risk for money laundering. . . . Riggs did not implement an effective system to identify and assess the BSA/AML risk present throughout the institution.\textsuperscript{37}

With regard to testing – the second required component of a BSA program – the OCC found that the bank’s system of testing for BSA compliance was inadequate: “Bank audits did not review all of the necessary areas, did not uncover or disclose the severity or the extent of


\textsuperscript{36.} OCC Consent Order 2004-44, \textit{supra} note 34, at 3.

\textsuperscript{37.} FinCEN Riggs Assessment, \textit{supra} note 35, at 2.
weaknesses in the Bank's BSA compliance, and contained flawed testing and sampling.\textsuperscript{38} Similarly, FinCEN determined that the "independent testing for compliance with the BSA was neither timely nor effective for the level of risk within Riggs."\textsuperscript{39}

Along these same lines, the OCC and FinCEN found the bank to be in non-compliance with the last two components required of a BSA program: designation of a compliance officer and training. With regard to the former, it was determined that:

Riggs also lacked effective monitoring for compliance by the BSA officer. Day-to-day oversight and monitoring of high-risk transactions, high-risk customers, and high-risk geographies were minimal. Strategies and alternative measures to ensure ongoing BSA/AML monitoring for suspicious transactions were not adequately developed and applied.\textsuperscript{40}

It is important to note here that the OCC's and FinCEN's criticisms of the bank's BSA compliance program were not made in a vacuum. As set forth in the OCC's Consent Order with Riggs, the bank's deficiencies contributed to the bank's failure to properly detect, investigate and file complete and accurate SARs.\textsuperscript{41} In addition, the bank did not adequately monitor for "suspicious cash, wire, or monetary instrument transactions"\textsuperscript{42} and, as a result, failed to identify or monitor potentially suspicious activity pertaining to:

- tens of millions of dollars in cash withdrawals from accounts related to the Saudi Arabian embassy;

- dozens of sequentially-numbered international drafts that totaled millions of dollars, that were drawn from accounts related to officials of Saudi Arabia, and that were returned to the bank;

\textsuperscript{38} OCC Consent Order 2004-44, \textit{supra} note 34, at 4.
\textsuperscript{39} FinCEN Riggs Assessment, \textit{supra} note 35, at 3.
\textsuperscript{40} \textit{Id.} at 4.
\textsuperscript{41} OCC Consent Order 2004-44, \textit{supra} note 34, at 5.
\textsuperscript{42} \textit{Id.}
• dozens of sequentially-numbered cashier's checks that were
drawn from accounts related to officials of Saudi Arabia
made payable to the account holder;

• millions of dollars deposited into a private investment
company\textsuperscript{43} owned by an official of Equatorial Guinea, a
small county on the west coast of Africa;

• hundreds of thousands of dollars transferred from an
account for Equatorial Guinea to the personal account of a
government official of that country; and

• over a million dollars transferred from an account for
Equatorial Guinea to a private investment company owned
by Riggs' relationship manager responsible for monitoring
the Equatorial Guinea accounts.\textsuperscript{44}

While the above information is set forth fairly graphically in the
OCC's and FinCEN's relatively short documents, the Minority Staff of
the U.S. Senate's Permanent Subcommittee on Investigations ("PSI")
set forth the issues at the bank in much more detail in its 113 page
report entitled "Money Laundering and Foreign Corruption:
Enforcement and Effectiveness of the Patriot Act; Case Study Involving
Riggs Bank."\textsuperscript{45}

With regard to the bank's handling of Equatorial Guinea, the
PSI report drew the following negative conclusions:

\textsuperscript{43} Riggs Statement of Offense, \textit{supra} note 2, at 8. As noted in the
Department of
Justice's Statement of Offense, "The OCC, in its Bank Secrecy Act/Anti-Money Laundering
Comptroller's Handbook, described the special risks involved with PICs: 'PICs are
incorporated frequently in countries that impose low or no taxes on company assets and
operations or are bank secrecy havens. \textit{Id.} Banks should exercise extra care when dealing
with beneficial owners of PICs and associated trusts because they can be misused to
camouflage illegal activities.'" \textit{Id.}

\textsuperscript{44} OCC Consent Order 2004-44, \textit{supra} note 34, at 6.

\textsuperscript{45} MINORITY STAFF OF THE PERMANENT SUBCOMM. ON INVESTIGATIONS, COMM. ON
GOV'T AFFAIRS, 108TH CONG., REPORT ON MONEY LAUNDERING AND FOREIGN
CORRUPTION: ENFORCEMENT & EFFECTIVENESS OF THE PATRIOT ACT—CASE STUDY
INVOLVING RIGGS BANK (COMM. PRINT 1950), \textit{available at} http://hsgac.
The Subcommittee investigation...determined that, from 1995 until 2004, Riggs Bank administered more than 60 accounts and CDs for the Government of Equatorial Guinea (E.G.), E.G. government officials, or their family members. By 2003, the E.G. accounts represented the largest relationship at Riggs Bank, with aggregate deposits ranging from $400 to $700 million at a time. The Subcommittee investigation has determined that Riggs Bank serviced the E.G. accounts with little or no attention to the bank’s anti-money laundering obligations, turned a blind eye to evidence suggesting the bank was handling the proceeds of foreign corruption, and allowed numerous suspicious transactions to take place without notifying law enforcement. . . . Riggs . . . over a three year period, from 2000 to 2002, facilitated nearly $13 million in cash deposits into Riggs accounts controlled by the E.G. President and his wife. On two of those occasions, Riggs accepted without due diligence $3 million in cash deposits for an account opened in the name of the E.G. President’s offshore shell corporation, Otong, S.A. . . . Riggs subsequently allowed wire transfers withdrawing more than $35 million from the E.G. government account, wiring the funds to two companies which were unknown to the bank and had accounts in jurisdictions with bank secrecy laws. . . . The senior leadership at Riggs Bank were well aware of the E.G. accounts and met on several occasions with the E.G. President and other E.G. officials. The bank leadership permitted the account manager handling the E.G. relationship to become closely involved with E.G. officials and business activities, including advising the E.G. government of financial matters and becoming the sole signatory on an E.G. account holding substantial funds. The bank exercised such lax oversight of the account manager’s activities that, among other misconduct, the account manager was able to wire
transfer more than $1 million from the E.G. oil account at Riggs to another bank for an account opened in the name of Jadini Holdings, an offshore corporation controlled by the account manager’s wife.\textsuperscript{46}

PSI also noted that Riggs continued to do business with Equatorial Guinea with inadequate oversight and controls in spite of the fact “Riggs was clearly aware of the corruption concerns associated with Equatorial Guinea.”\textsuperscript{47} In addition, PSI pointed out that $11.5 million of the cash deposits referenced above, that were made on behalf of the President of Equatorial Guinea, were actually physically brought into the bank on six different days over the course of two years by the Riggs officer who was the relationship manager for the Equatorial Guinea accounts.\textsuperscript{48} The cash was brought into the bank in increments of $1-$3 million in “unopened, plastic-wrapped bundles.”\textsuperscript{49} PSI estimated that the $3 million in cash weighed approximately 60 pounds.\textsuperscript{50} So, according to the PSI report, there was an account relationship manager depositing 60 pounds of shrink-wrapped cash on a periodic basis on behalf of a bank customer with no explanation or review or after-the-fact analysis or audit. And this was the account manager who had the authority to wire transfer more than $1 million from an Equatorial Guinea account to another bank and over whom there was very “lax oversight.”\textsuperscript{51} This, unfortunately, was a formula for disaster and Riggs has had to pay a severe price.

On behalf of the bank, it should be noted that it was well aware of the Equatorial Guinea account relationship and, in 2001, as the PSI report noted, “several senior Riggs Board members and bank officers formed a high level committee which met quarterly each year to provide special attention to the E.G. relationship.”\textsuperscript{52} However, it would appear that the “high level committee” provided inadequate oversight for the relationship and focused, perhaps, too much on how to grow the account

\begin{footnotes}
\item[46] Id. at 3-4.
\item[47] Id. at 46.
\item[48] Id. at 51.
\item[49] Id. at 51. Shades, unfortunately, of UBS are clearly very suspicious.
\item[50] PSI report, supra note 45, at 51.
\item[51] Id. at 4.
\item[52] Id. at 64.
\end{footnotes}
The supervision and understanding of the account relationship was so poor that, when the OCC asked for information about the accounts and, later, when PSI subpoenaed the account information, the bank could find and produce information for only 30 of the 60 existing accounts for Equatorial Guinea. It took the OCC examiners to find the other 30 accounts. Further, even though the underlying transactions in the accounts were suspicious and the size and nature of the relationship were questionable, Riggs did not identify the accounts as high risk until October, 2003, several months after the initial consent cease and desist order was entered into by the bank with the OCC to address BSA issues.

As set forth in the OCC and FinCEN documents and in the PSI report, Riggs—in spite of the high risk nature of the accounts, the possibility that the bank was assisting public corruption of behalf of a foreign dictator and his family, and the various suspicious transactions that occurred in the account relationship—failed to identify or monitor the risk, failed to file required SARs with regard to the account relationship and failed to provide sufficient supervision over the account relationship manager.

Further, once these issues were brought to the bank’s attention, members of the board indicated an unwillingness to consider closing the accounts. As late as December 17, 2003, Director Joseph Allbritton was quoted as saying that “the bank had no intention of closing the E.G. accounts.”

In addition to the Equatorial Guinea account relationship, the PSI report focused on Riggs’ account relationship with Augusto Pinochet, the former President of Chile, and drew these negative conclusions:

53. See id.
54. Id. at 66; OCC Consent Order 2004-44, supra note 34, at 4; FinCEN Riggs Assessment, supra note 35, at 3.
55. PSI report, supra note 45, at 66.
56. Id. at 4.
58. PSI report, supra note 45, at 66, 72.
59. Id. at 67, 83.
The evidence obtained by the Subcommittee staff shows that, from 1994 until 2002, Riggs Bank (Riggs) opened at least six accounts and issued several certificates of deposit (CDs) for Augusto Pinochet, former President of Chile, while he was under house arrest in the United Kingdom and his assets were the subject of court proceedings. The aggregate deposits in the Pinochet accounts at Riggs ranged from $4 to $8 million at a time. The Subcommittee investigation had determined that the bank’s leadership directly solicited the accounts from Mr. Pinochet, and Riggs account managers took actions consistent with helping Mr. Pinochet to evade legal proceedings seeking to discover and attach his bank accounts. The Subcommittee investigation found that Riggs opened multiple accounts and accepted millions of dollars in deposits from Mr. Pinochet with no serious inquiry into questions regarding the source or his wealth; helped him set up offshore shell corporations and open accounts in the names of those corporations to disguise his control of the accounts; altered the names of his personal accounts to disguise their ownership; transferred $1.6 million from London to the United States while Mr. Pinochet was in detention and the subject of a court order to attach his bank accounts; conducted transactions through Riggs’ own accounts to hide Mr. Pinochet’s involvement in some cash transactions; and delivered over $1.9 million in cashiers checks to Mr. Pinochet in Chile to enable him to obtain substantial cash payments from banks in that country. The Subcommittee investigation also determined that Riggs concealed the existence of the Pinochet accounts from OCC bank examiners for two years, initially resisted OCC requests for information, and closed the accounts only after a targeted OCC examination in 2002.60

60. Id. at 2-3.
Riggs Bank assisted Augusto Pinochet, former president of Chile, to evade legal proceedings related to his Riggs bank accounts and resisted OCC oversight of these accounts, despite red flags involving the source of Mr. Pinochet's wealth, pending legal proceedings to freeze his assets, and public allegations of serious wrongdoing by this client.\textsuperscript{61}

On March 24, 1999, the Law Lords authorized an extradition hearing to determine whether Mr. Pinochet should be transferred to Spain. Two days later, on March 26, 1999, Riggs allowed Mr. Pinochet to prematurely terminate the 1 million pound CD held in the name of Althorp at Riggs in London, and transfer the funds, totaling $1.6 million in U.S. dollars, to a new CD in the United States.\textsuperscript{62}

In spite of this litany, the bank, according to the PSI report, again resisted closing the accounts. Specifically, Mrs. Allbritton, a member of the bank's board, allegedly "complained to the OCC about losing the Pinochet accounts."\textsuperscript{63} As set forth by the PSI report with regard to both the Pinochet and the Equatorial Guinea accounts:

The corporate culture at Riggs failed to communicate the importance of the bank's anti-money laundering program. The Subcommittee was told that the bank's senior leadership clearly valued the Embassy accounts and accounts opened for foreign leaders. . . . The 1994 trip to Chile by senior Board members to solicit the Pinochet account and the 2001 luncheon in honor of the Equatorial Guinea president illustrate the Board's personal involvement in these accounts. In 2002 and 2003, some Board members expressed opposition to closing the Pinochet and Equatorial Guinea accounts

\textsuperscript{61} \textit{Id.} at 7.
\textsuperscript{62} \textit{Id.} at 29 (footnotes omitted).
\textsuperscript{63} PSI report, \textit{supra} note 45, at 81.
due to money laundering concerns. In March 2003, senior bank officers complained to the OCC about forcing the bank to adopt a rigorous AML program. These are not the actions or sentiments of a Board committed to AML excellence. 64 

The bank’s failure to establish and to adhere to an adequate BSA program led not only to two cease and desist orders against the bank and an extremely large civil money penalty, it also had other ramifications. Specifically, on January 27, 2005, Riggs Bank pled guilty to one count of violating 31 U.S.C. §§ 5322 and 5318(g) for failure to file timely and accurate SARs with regard to the Equatorial Guinea and the Pinochet matters detailed above. 65 Many of the deficiencies involving Pinochet’s accounts noted by the OCC, FinCEN and PSI were also detailed in the Department of Justice’s Statement of Offense. 66 For instance, the Department of Justice noted that Riggs maintained numerous accounts for Equatorial Guinea and its senior government officials; that the relationship was the bank’s single largest, with balances and loans totaling nearly $700 million; that there were many allegations of corruption and abuse by the country’s government; and that there were numerous, suspicious, transactions involving the Equatorial Guinea accounts. 67 Similarly, the Department of Justice noted that, by March, 2000, Pinochet had been the subject of warrants alleging human rights crimes issued by Spain, Switzerland, Belgium and France and that, by October, 1998, a Spanish magistrate had issued an “arrest warrant for Pinochet for crimes of genocide, terrorism and torture.” 68

As a result of Riggs’ misconduct and failure to file SARs with regard to the suspicious activity detailed above, the Department of Justice assessed a criminal fine against the bank in the amount of $16

64. Id. at 73.
66. See generally Riggs Statement of Offense, supra note 2.
67. Id. at 8.
68. Id. at 4.
As with UBS, the Riggs case is unusual. The case involved a unique bank with a heavy concentration of embassy banking. In addition, Riggs clearly had some customers who were “politically exposed persons” or “PEPs.” Along with that, there were allegations of public corruption and there was a large volume of cash and international transactions. These are not common attributes for an average U.S. domestic bank. However, in spite of this, as with the UBS case, there are a number of lessons to be learned.

First and foremost, regardless of the bank’s level of risk, it is essential for the bank to fully understand its risks and, second, for the bank to ensure that it can manage those risks. In order to do that, the bank must know the specific risks that are associated with all of its products, services and customers. This requires well-documented account opening procedures, strong customer identification processes and effective monitoring systems. If the bank does not have adequate policies and procedures, it will not be able to perform these functions. Similarly, if the essential components of an adequate BSA program are missing, it will lead to problems. Further, if the willingness and ability of the staff and senior management to review potentially suspicious transactions are lacking, the bank will be left unprotected. Most importantly, if the leadership and the culture created by senior management and by the board of directors are not sufficiently focused on compliance, the rest of the bank will be lax and problems will inevitably result.

As reflected in both the UBS case and in the Riggs case, having sufficient internal controls, audit and training are essential. If a bank loses sight of its obligations to its shareholders and its responsibilities for complying with laws, rules and regulations, as well as safe and sound banking practices, and turns a blind eye to the potential wrongdoing or suspicious conduct of certain customers, it is creating an irreconcilable conflict. A bank cannot blindly serve its customers and be able to adhere to its other responsibilities at the same time.

---

70. PSI report, supra note 45, at 13.
71. See 31 C.F.R. § 103.175(o) (2004).
IV. CRIMINAL ENFORCEMENT ACTIONS UNDER THE BSA

Although the BSA has provided for criminal penalties for over thirty years, only five banks have faced criminal action based on the failure to file SARs. However, the existence of these cases has created concern as to whether there will be a continued increase in such cases and whether these cases have been appropriate.

A. Broadway Case

The first case involving a criminal sanction against a bank for failure to file a SAR involved Broadway National Bank, New York, New York. In that case, the bank pled guilty to three criminal counts – failure to establish or maintain an adequate BSA program, failure to file SARs and affirmatively assisting customers in structuring cash deposits in order to evade the BSA reporting requirements. The bank also paid a criminal fine of $4 million.

There was little to no adverse reaction to the criminal plea in the Broadway case and that was, perhaps, because of the overwhelming egregiousness of the case. As set forth in the United States Attorney’s Office’s press release, the case involved thousands of bulk cash and structured deposits at the bank over a two-year period. The deposits totaled approximately $123 million. In addition, while the bank was well aware of the deposits, it never investigated them or filed the necessary SARs.

The bulk deposits were made primarily by one customer, a Mr. Alfred Dauber, who had his runner deliver the cash to the bank in duffel bags “filled with hundred[s] of thousands of dollars in small bills, wrapped in rubber bands.” Almost as part of a bad caricature of a money launderer, the runner would not even wait for the cash to be

73. Broadway Press Release, supra note 72.
74. Id.
75. Id.
76. Id.
counted, but, rather, would leave the duffel bag at the bank and pick it up – along with his receipt – the next time he made his deposit run to the bank.\textsuperscript{77} The money was so voluminous that the tellers had to work through their lunch hours to count it and they continuously complained to senior bank management.\textsuperscript{78} In spite of that, the senior management not only failed to investigate or put an end to the transactions, they approved the prompt wiring of the funds to Columbia, Panama and Miami.\textsuperscript{79} One of the senior managers approving the wiring of these funds was also the bank’s BSA compliance officer.\textsuperscript{80} To make matters even more suspicious, the cash that the runner periodically dropped off at the bank often did not match the amounts listed on the deposit slips.\textsuperscript{81} In this fashion, Dauber made 250 deposits of bulk cash totaling approximately $46 million.\textsuperscript{82} And yet the bank never investigated Dauber or his transactions.\textsuperscript{83}

Dauber claimed that he was involved in the “electronics business,” but the bank did nothing to verify this.\textsuperscript{84} Dauber claimed that his business was only a few blocks from the bank, but the bank never inspected the site.\textsuperscript{85} In other words, the bank allowed its staff to be tied up in counting hundreds of thousands of dollars, allowed management to immediately wire the funds to well-known money laundering havens (thus, not even getting the use of the money), processed $46 million deposited in cash in the most suspicious way, failed utterly to verify the identity of the customer or the true nature of his business and generally failed to implement a protective anti-money laundering program.

In addition to mishandling the Dauber account relationship, the bank permitted a number of customers to engage in structuring deposits, which is the practice of making cash deposits just under the $10,000 threshold in order to evade the reporting requirements for cash

\begin{itemize}
\item \textsuperscript{77} Id.
\item \textsuperscript{78} Broadway Press Release, supra note 72.
\item \textsuperscript{79} Id.
\item \textsuperscript{80} Government’s Sentencing Memorandum at 10, 17, U.S. v. Broadway National Bank, (2002) (02 Cr. 1507 (TPG)) (on file with author and NCBI).
\item \textsuperscript{81} Information at 12, U.S. v. Broadway National Bank, (2002) (02 Cr. 1507 (TPG)) (on file with author and NCBI).
\item \textsuperscript{82} Broadway Press Release, supra note 72.
\item \textsuperscript{83} Id.
\item \textsuperscript{84} Id.
\item \textsuperscript{85} Id.
\end{itemize}
transactions pursuant to the BSA. All tolled, there were thousands of structured deposits that totaled approximately $76 million over the course of two years.

One particular account relationship, involving the Fares family, was of note and was detailed in the United States Attorney's Press Release and Sentencing Memorandum. Drawing from examples relating to the Fares' accounts, it was noted that, on one particular day, January 16, 1998, the Fareses deposited over $167,000 into 17 different accounts, using nothing but cash deposits of just under $10,000. Further, on March 16, 1998, the Fareses make 12 different cash deposits, all ranging between $8,990 and $9,900. On the very next day, they made another 12 cash deposits, 11 of which were between $9,600 and $9,900, with one at $8,500. On the third day, they made five more cash deposits, four between $9,650 and $9,800, and one at $8,000. In spite of the incredibly obvious nature, volume and frequency of the structuring, the bank further aggravated the situation by promptly wiring the funds to Panama and Lebanon. In addition, the bank ignored the fact that the accounts were linked (in the sense of having the same addresses, the same company officers and the same account signers), that the deposits were made into different accounts, but all at the same time, and that the primary business address for most of the accounts was a small storefront directly across the street from the bank that could not possibly have legitimately generated the volume of cash that was deposited on a regular basis into the bank. The bank, however, with one exception, failed to file any SARs and filed only a few CTRs in connection with the Fares' accounts. To aggravate the situation, Broadway had failed to implement an effective BSA program.

86. Id.
88. Id.
89. Government’s Sentencing Memorandum, supra note 80, at 20.
90. Id. at 21.
91. Id.
92. Id.
95. Id. at 22. The one SAR that was filed was two years before the activity set forth in the Sentencing Memorandum and occurred only because the bank's outside auditors identified it and directed the bank to make the filing. Id.
despite warnings from banking regulators and Broadway’s outside auditors.96

In summary, as the United States Attorney for the Southern District of New York, James B. Comey, said, “Broadway National Bank utterly failed to implement any program at all, let alone an effective one, with the dire result that over approximately $123 million in narcotics proceeds was laundered through the bank.”97 This fact alone makes the Broadway case an outlier. Most banks, as Mr. William Fox, the Director of FinCEN, has stated, “have good systems in place.”98 Thus, the severe actions, administrative or criminal, appear to be brought primarily against banks that, in Mr. Fox’s description, have clear BSA system failures, “systems that were nonexistent or weak.”99 Clearly, in order to avoid the mistakes committed by Broadway, banks must have strong and effective BSA compliance programs, good internal controls, sufficient monitoring of accounts and transactions, adequate training, and a program for knowing their customers and the nature of their businesses. In addition, the Board and senior management must have a willingness and ability to identify the bank’s high risk customers, services and products and to properly manage the associated risks.

B. Banco Popular Case

The second case that resulted in a criminal action for the failure to file a SAR involved Banco Popular de Puerto Rico. In that case, the bank agreed to a year-long deferred prosecution and paid a civil forfeiture of $21.6 million.100 The bank also agreed to pay a $20 million civil money penalty assessed by FinCEN, which was deemed to be satisfied by the $21.6 million forfeiture.101 The facts that justified this action were serious and stemmed from the bank’s lack of monitoring and failure to react to the “voluminous unusual or suspicious

96. Id. at 7-14.
99. Id.
101. Id. at 3.
transactions” of two customers, as well as from the fact that the bank was servicing a number of foreign money service businesses located in the Dominican Republic without sufficient appreciation for the risk and without conducting adequate due diligence.102

With regard to the first customer, Roberto Ferrario Pozzi, the bank recorded him as having four different types of businesses: (1) selling phone cards and long distance telephone, facsimile and money transmission services; (2) managing a gas station; (3) operating a café by the name of “Gilligans;” and (4) running a business mysteriously entitled “Puerto Rico Net Yellow.”103 However, the bank never bothered to determine which, if any, of these lines of business were accurate or legitimate. So, from the beginning, the bank had no idea who its customer was.

On top of that, during the course of a three year period, from June 1995 to March 1998, the customer deposited $20 million in cash.104 Over the next six months, between March 1998 and September 1998, Ferrario deposited another $8 million in cash.105 The cash deposits frequently totaled hundreds of thousands of dollars in a single day and the monthly total of deposits went from $34,000 in August 1995, to an average of $1.4 million for the last six months of 1997.106 Similar to Mr. Dauber in the Broadway case, Ferrario on occasion brought the money into Banco Popular in gym bags.107 And, similar to the Broadway case, because Ferrario’s deposits were in small denominations, his activity succeeded in disrupting the operations of Banco Popular due to the time it took the tellers to count the cash.108 Management, in fact, was aware of this problem and discussed it at monthly meetings, but did nothing.109

In addition to the high volume and very unusual nature and

102. See id. at 15.
103. Id. at 16.
104. Id.
106. Id. at 16-17. What was almost humorous is the fact that, in one single week in 1995, the same employee filed three different CTRs with regard to Ferrario’s deposits and listed three separate sources for the funds – “overseas calls, gas station, and money transfer.” Id. at 18-19.
107. Id. at 16.
108. See id. at 17.
109. See id. at 19.
growth of the cash deposits, Ferrario regularly wired out his funds on the same day, or within one day, of the deposit. This wire activity was so substantial that it represented 25% of a particular branch's wire activity. To make the activity even more suspicious, the wires were sent to 300 different companies or individuals. One has to wonder how many gas stations, local cafes, or even "Net Yellow" companies would require that much wire activity. And yet the bank did not investigate.

As early as October 1995, an employee told a branch manager that the transactions were significant and suspicious and yet the bank did nothing. In addition, tellers commented that the money deposited by Ferrario was "strange or unusual," and yet the bank did nothing. Further, bank employees regularly walked by Ferrario's purported place of business on the way to and from work and "rarely saw customers at the business."

It was not until December 1997, over two years after Ferrario's suspicious activity began, that the bank started to investigate. And it was not until March 1998, that the bank filed its one and only SAR, which was incomplete and inaccurate.

As if Banco Popular's poor record with regard to Ferrario was not enough, the bank had similar failures with regard to a second customer, Jairo de Jesus Vallejo, who maintained accounts for two different businesses. In the one account, the average monthly balance went from $3,000 to $120,000 in less than one year, representing a 40-fold increase. In addition, the nature of the deposits into the account went from being primarily checks to consisting mostly of cash, which

111. Id.
112. Id.
113. Id. at 17-18.
114. Id. at 17.
116. Id.
117. Id. at 18-19.
118. See id. at 16, 19-20.
119. Id. at 15, 21.
was, according to the Deferred Prosecution Agreement, inconsistent with Vallejo’s stated business for this account – distributing hydraulic equipment.\(^{121}\)

Further, the cash deposits themselves were suspicious and clearly involved structuring.\(^{122}\) Vallejo made as many as six deposits a day at multiple branches, all in amounts under the CTR $10,000 limit.\(^{123}\) In fact, the bank’s systems identified the structuring, but the bank did not file a SAR.\(^{124}\) In closing its investigation into the matter, the bank noted that the activity stopped, but it had not.\(^{125}\)

By the time the bank finally did file SARs on Vallejo’s two accounts, over $1 million had passed through the accounts, which the bank subsequently learned were the proceeds of narcotics trafficking.\(^{126}\) However, as noted in the Deferred Prosecution Agreement, the SARs were incomplete in that they did not fully describe the amount of the activity or the length of time during which the activity was conducted.\(^{127}\)

In addition to the bank’s deficiencies with regard to monitoring the suspicious nature of high-risk, cash-oriented, individual customers, Banco Popular, for over three years, provided correspondent services to high-risk foreign money service businesses (“MSBs”) located in the Dominican Republic.\(^{128}\) The specific problems in this area were threefold. First, the bank engaged in this high-risk business without adequately reviewing and documenting the nature and extent of the MSBs’ activity.\(^{129}\) Second, the bank processed checks for the MSBs on a bulk basis without reviewing the transactions for suspicious activity.\(^{130}\) Had it done so, the bank might have been able to identify that the activity was indicative of money laundering.\(^{131}\) Third, the bank allowed suspicious activity to continue without adequate investigation or

---

121. Id.
122. See id.
123. Id.
124. Id. at 22.
126. Id. at 23.
127. Id.
128. Id. at 24.
129. Id. at 24-25.
131. Id.
analysis even after the bank was specifically put on notice by law enforcement. In one instance, the Drug Enforcement Administration issued a warrant seizing $275,000 from an account at the bank. On the very same day, the bank allowed the account holder's brother to open another account specifically so that it could serve as a substitute for the account that had just been seized and closed. This failure to respond to information provided from outside sources, particularly law enforcement, was also a contributing problem for the bank with regard to its handling of both the Ferrario and Vallejo accounts. With regard to both individuals, the bank received law enforcement subpoenas, but ignored the obvious need to conduct an independent review of the accounts that were being subpoenaed.

Thus, the Banco Popular case reinforces the need for banks to have good customer identification programs, systems to monitor for suspicious transactions and activity, and procedures to follow up and investigate suspicious activity and the concerns of the officers and employees of the bank. The bank must also establish procedures to ensure the coordination and communication necessary to review transactions and accounts that are potentially the subject of law enforcement inquiry. Lastly, the bank must have the ability to understand the risks involved with regard to the products, services and customers of the bank, and the culture and support to ensure that the bank has the personnel, knowledge, ability, willingness and internal controls to manage those risks.

C. Delta Case

In the third criminal case, Delta National Bank, New York, New York, pled guilty to a one-count information for failure to file a SAR and agreed to forfeit $950,000. Unlike the other cases described above that involved criminal cases against banks for the failure to file SARs, the Delta National Bank case is difficult to understand. While

132. Id.
133. Id.
134. Id. at 19, 22.
the bank clearly acknowledged wrongdoing in the plea agreement, the basis for the plea is unclear.

The U.S. Attorney's Press Release says that Delta National Bank pled guilty to "one count of failure to file a Suspicious Activity Report (SAR) in connection with the use of a customer's account for foreign exchange business, including a June 28, 2000, transaction made between two accounts at the bank." As set forth in slightly more detail later on in the page and one-half press release, the U.S. Attorney's Office stated:

According to the plea agreement, the Customer assisted other Colombian customers of Delta National with transactions in their accounts that were conducted as part of the foreign currency exchange business. Delta National was aware of this assistance. Delta National agreed that the government could produce evidence to prove that the total amount involved in the Customer's foreign currency exchange transactions was between $5 million and $10 million.

The corresponding press release issued by U.S. Immigration and Customs Enforcement (ICE) had the identical language, except for the addition of two phrases highlighted here in italics:

According to the plea agreement, the Customer assisted other Colombian customers of Delta National with transactions in their accounts that were conducted as part of the foreign currency exchange business. Delta National was aware of this assistance. Delta National agreed that the government could produce evidence to prove that the total amount involved in the Customer's foreign currency exchange transactions that required reporting was between $5 million and $10 million.

Delta failed to file these reports.

136. Id.
137. Id.
Analyzing the U.S. Attorney’s Press Release, it is difficult to determine what is criminal about a bank having a customer who, in turn, assisted one of its own customers in conducting a “foreign currency exchange business.” While, clearly, there could have been something criminal related to this matter, the press release does not seem to explain it. The additional language in the ICE press release at least intimates that there were reports to be filed that were not. However, the ICE press release does not explain why the reports (presumably SARs) should have been filed.

Unfortunately, the U.S. Attorney’s criminal information does not shed much light, saying that the bank:

did knowingly and willfully fail to file a Suspicious Activity Report . . . pertaining to a June 28, 2000, book transfer of $50,000 from an account at Delta National Bank and Trust Company and into account number 600822, which was held at Delta National Bank and Trust Company under the name ‘Vanina.’

It is unclear why the failure to file a solitary SAR involving the internal book transfer of $50,000 from one account to another is indicative of criminal misconduct.

The Statement of Facts, or Allocution, in the case stated the following and only assists the analysis marginally:

- The transaction at issue was part of a pattern of activity involving more than $100,000 in a 12-month period.

- The value of the funds involved, according to the government’s evidence, was more than $5 million and less than $10 million.


• The Bank knew, suspected, or had reason to suspect that the transaction identified in the Information had no business purpose.

• The Information identifies a transaction for which the Bank willfully did not file a Suspicious Activity Report.

• The Bank did not know that the funds were the proceeds of unlawful activity, but acted with reckless disregard of the source of the funds.

• Foreign currency exchange businesses in Colombia have been identified by the Bank's primary regulator, the Office of the Comptroller of the Currency, and other federal agencies as "high risk" for the involvement of money laundering of the proceeds of narcotics trafficking and other criminal activity. During the period mentioned in the Information, the Bank and its officers were aware of these risks, and were aware that the Customer was operating such a business.

• During the period mentioned in the Information, the Customer assisted other Colombian customers of the Bank with transactions in their accounts that were conducted as part of the foreign currency exchange business, and the Bank was aware of this assistance.

• The Bank agrees that if this case had gone to trial, the government could produce evidence to prove that two such transactions, conducted as part of the foreign currency exchange business, were a $50,000 book transfer on June 28, 2000, and a $65,000 book transfer on July 10, 2000.

• The bank acknowledges that a Suspicious Activity Report was required to be filed concerning the use of the Customer's account for foreign currency exchange business, including the two transactions described above.
The Bank incorrectly concluded that no Suspicious Activity Report was required, and, thus, willfully failed to file a report in violation of the law.\textsuperscript{140}

First, there is mention of a pattern of conduct involving $100,000 and an overall value of some unspecified funds ranging from $5 million to $10 million. However, there is no explanation (as there is in the other criminal cases described above) what these amounts pertain to. Further, there is no explanation as to how these relatively large amounts relate to the relatively small, one-time transfers involving $50,000 and $65,000, only one of which is referenced in the criminal information. Granted that the failure to file a SAR when one “knew, suspected, or had reason to suspect that the transaction identified in the Information had no business purpose” is a violation of the regulatory requirements set forth in 12 C.F.R. § 21.11(c)(4)(iii), it is still unclear why this rose to the level of a criminal case. This is especially the case when the Information also states that the “Bank did not know that the funds were the proceeds of unlawful activity, but acted with reckless disregard of the source of the funds.”\textsuperscript{141} Specifically, it is not explained in what way the bank may have engaged in “reckless disregard.” Further, the fact that the particular customer – or, more specifically, the customer’s line of business – is high-risk does not mean that a bank cannot have such a customer as a client. It simply means that the bank has to have identified the risk (which, according to the Information, the bank had done), understood the risk, and established adequate procedures for supervising and managing the risk. It is unclear how the bank failed to perform these latter functions and why, assuming it had failed, it became a criminal matter. Again, while it is clear that the bank pled guilty to willfully failing to file a SAR, it would have been preferable to be able to understand what the bank specifically did or did not do that created criminal liability. What is particularly troubling is the fact that the very last sentence in the Appendix to the Statement of Fact (or Allocution) is: “During the period mentioned in the Information, the Bank incorrectly concluded that no Suspicious Activity


\textsuperscript{141} Id. at 4-5.
Report was required, and thus willfully failed to file a report in violation of the law. Ordinarily, an incorrect conclusion, absent aggravating factors, as to whether to file a SAR, does not and should not create criminal liability. In this case, it is unclear what the aggravating factors might have been.

As set forth in two articles at the time of this action, the bank claimed that: "Prior to this matter, we enjoyed an unblemished regulatory record, about which we are very proud." These articles also say the following about the case:

A New York bank agreed...to forfeit $950,000 for failing to report a series of suspicious transactions that federal authorities said could have helped fuel a vast underground system used to launder international drug profits....The undercover investigation, dubbed Operation Laundry Chute, chiefly targeted Colombian drug traffickers who use a system known as the "Black Market Peso Exchange" to launder profits from illegal drug sales.

However, as set forth above, there is no mention of the "Black Market Peso Exchange" or of "a vast underground system" in the U.S. Attorney's press release, Information or Statement of Facts. Consequently, there is no way of knowing if these dramatic newspaper statements are accurate.

In addition, it is curious that The Miami Herald, in its story about the case, claimed the following:

According to the plea agreement, Delta National opened an account in 1998 at its Miami branch for a Colombian who operated a foreign-currency exchange business in Bogota. Such businesses in Colombia have been

142. Id. Attachment A, at 3.
identified by the U.S. government as high risk for involvement in money laundering. That classification required Delta National to file SARs on the account, but it failed to do so, according to an ICE news release.\textsuperscript{145}

The first two sentences may well be correct. The last sentence; however, is not. As stated above, the banking regulators do not impose prohibitions on whom a bank may have as a customer. Unfortunately, such news stories only serve to confuse matters.

It would appear that, due to the lack of details provided by the U.S. Attorney’s Office in the Delta case, there are not very many lessons, if any, to be learned. It is clear that there was some criminality alleged by the prosecutor and acknowledged by the bank, but it is not clear what the criminality, or the bank’s misconduct, was. The one lesson that, perhaps, can be deduced from this case is the importance of a bank knowing its customers and its customers’ businesses and the need for the bank to exercise enhanced due diligence with regard to all of its high-risk customers.

\section*{D. Amsouth Case}

Several months after the UBS and Riggs administrative cases, on October 12, 2004, the United States Attorney’s Office for the Southern District of Mississippi announced a settlement with AmSouth Bank, Birmingham, Alabama, consisting of the forfeiture of $40 million to the United States as part of a deferred prosecution agreement.\textsuperscript{146} On the same day, the Federal Reserve and FinCEN announced the joint assessment of a $10 million civil money penalty against the bank.\textsuperscript{147}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{145} Fields, \textit{supra} note 143, at 3C.
\end{itemize}
\end{footnotesize}
Again, the question is raised as to what caused such a large forfeiture and accompanying penalty?

The simple answer, as set forth in the U.S. Attorney's Deferred Prosecution Agreement, is that the bank pled guilty to "one count . . . of failing to file suspicious activity reports in a timely, complete and accurate manner, in violation of 31 U.S.C. §§ 5318(g)(1) and 5322(b) and 31 C.F.R. § 103.18.") However, the Statement of Facts that accompanied the Agreement and which the bank "accept[ed] and acknowledge[d]," reflects a more involved story.

This case, however, has been very controversial. Specifically, a former General Counsel of the Department of the Treasury, David Aufhauser, has termed the case "a hijacking of a regulatory issue."

In addition, William Fox, the Director of FinCEN, in referring to this case, has said that he had "very serious concerns about what appears to be a trend to criminalize behavior designed to be governed by civil standards." The concern voiced is perhaps based on the question that could be asked about the Delta case discussed immediately above. That question is whether the failure to file a single SAR (which is at first blush simply a regulatory requirement) or, alternatively, the failure to correctly conclude that a SAR is required to be filed, will or should result in criminal charges. This is a difficult issue, but – aside potentially from the Delta case – the other cases detailed in this article, including the AmSouth case, involved much more than the failure to file a single SAR.

As set forth in the Department of Justice's press release, the case emanates from the fact that the bank allowed $20 million to flow through its accounts in a Ponzi scheme that defrauded approximately 60 customers of their savings. In addition to not adequately performing


149. Id.


151. Id.

due diligence, the bank had in its possession – and was apparently aware of – promotional materials relating to the scheme which indicated that the investors were being promised an investment return of up to 25% a month\textsuperscript{153} – a virtual impossibility. It would appear that this should have been identified and reported as suspicious, especially in light of the amount of money involved. Further, according to the Department of Justice’s Statement of Facts, the bank engaged in questionable conduct by providing blank account opening documents to the two perpetrators of the scheme so that they could open accounts for individuals the bank did not meet and whose identities the bank did not verify.\textsuperscript{154} The bank further failed to comply with the instructions and restrictions set forth in the “Direction of Investment” forms signed by the underlying customers and, without the knowledge or consent of the customers, provided copies of their bank statements to the two perpetrators of the Ponzi scheme.\textsuperscript{155} Perhaps even more problematic was the fact that the bank refused or was unable to adequately respond to a series of grand jury subpoenas.\textsuperscript{156} Specifically, the bank “(i) failed to timely produce certain documents called for” by the grand jury subpoenas; “(ii) failed to produce certain documents in the manner they were kept in the regular course of business as required by the subpoenas; and (iii) failed to locate and produce certain documents called for by the subpoenas.”\textsuperscript{157} In fact, the bank failed to locate and produce certain documents until after it had become a target of the criminal investigation.\textsuperscript{158} Naturally, any bank that treats grand jury subpoenas in such a cavalier fashion is apt to be asking for problems. A similar lack of responsiveness was an issue in both the UBS and Riggs cases.

To make matters worse, according to the Department of Justice’s Statement of Facts, the bank’s inside counsel failed to search even his own files and did not bother to request documents of


\textsuperscript{154} Id. at 5.

\textsuperscript{155} Id. at 5-6.

\textsuperscript{156} Id. at 7-8.

\textsuperscript{157} Id. at 8.

\textsuperscript{158} Amsouth Statement of Facts, supra note 153, at 9.
employees he knew or should have known had responsive documents.  

Last, the bank’s outside counsel, according to the Statement of Facts, provided misleading responses to the U.S. Attorney’s Office in connection with the grand jury subpoenas and failed to ensure, even after “many discussions and other communications” with the U.S. Attorney’s Office, that the bank had produced all responsive documents on a timely basis. Again, this lack of responsiveness is a formula for disaster. Even if there is an argument that the action by the U.S. Attorney’s Office was inappropriate or somehow improperly crossed over into the “regulatory” arena, it is clear that AmSouth made a number of serious missteps and failed to respond to an ongoing grand jury investigation in a full, complete and cooperative fashion. No matter what trouble the bank has gotten into, or what defenses it might have, it is absolutely essential for it to cooperate with the U.S. Attorney’s Office and its regulators to the fullest extent possible.

According to the Federal Reserve’s press release, there were “systemic defects in AmSouth’s program with respect to internal controls, employee training, and independent review that resulted in failures to identify, analyze and report suspicious activity occurring at the bank.” In addition, in the Federal Reserve’s Cease and Desist Order and Order of Assessment of a Civil Money Penalty, the “whereas” clauses recite that the bank: (a) failed to “establish and maintain procedures reasonably designed to [ensure] and monitor compliance with the BSA;” (b) failed to “file accurate, complete, or timely Suspicious Activity Reports;” and (c) failed “to have adequate systems in place to prevent, identify, and report criminal activity . . . and [failed] to promptly and fully cooperate with law enforcement authorities . . . .” Similarly, FinCEN’s Assessment of Civil Money Penalty stated that:

AmSouth willfully violated the anti-money laundering program and suspicious activity reporting requirements of the Bank Secrecy Act and its implementing regulations. AmSouth failed to develop an anti-money
launding program tailored to the risks of its business and reasonably designed, as required by law, to prevent the Bank from being used to launder money and finance terrorist activities and to ensure compliance with the Bank Secrecy Act. AmSouth's program lacked adequate board and management oversight, lacked fully implemented policies and procedures across the Bank to provide for appropriate due diligence and capture of suspicious activity information, lacked adequate training to ensure compliance, and had a materially deficient internal audit process that failed to detect these inadequacies. The result was a fragmented program in which areas of the Bank had information on suspicious activity that was never communicated to those responsible for Bank Secrecy Act compliance. FinCEN has determined that AmSouth's program was materially deficient in three of the four required elements: internal controls, training, and audit.\footnote{163. FinCEN Amsouth Assessment, \textit{supra} note 147, at 1-3.}

This is a very poor record and is reflective of the lack of internal controls and adequate BSA program alleged to have existed at UBS, Riggs, Broadway and Banco Popular.

In addition, AmSouth had no system in place to alert BSA compliance personnel to the existence of subpoenas, and the bank had no policies and procedures to ensure the referral, investigation and reporting of suspicious activities.\footnote{164. \textit{Id.} at 3-4.} These deficiencies became important with regard to the specific matter that gave rise to the forfeiture and penalty because the two men running the Ponzi scheme were relatively well-known to the bank; employees and officers in seven different branches in four different states had contact with the two individuals during the course of the scheme.\footnote{165. Amsouth Statement of Facts, \textit{supra} note 153, at 11.} Further, at least one employee had suspicions that there was an illegal scheme being perpetrated and reported his concerns to both the bank's legal department and Corporate Security department.\footnote{166. \textit{Id.}} Yet neither of these
In addition to the failure by AmSouth to identify, investigate and/or report the Ponzi scheme that was at the heart of the criminal and administrative case, it should be noted that both the U.S. Attorney’s Statement of Facts and the FinCEN Assessment of a Civil Money Penalty recite a series of four to eight instances in which the bank failed to report other known or obvious suspicious transactions. Some of these transactions involved millions of dollars and reflect the bank’s failure to respond to or investigate the concerns of bank employees, as well as very basic flaws in the bank’s training program. On the latter point, it was noted in the Statement of Facts and the FinCEN Assessment that AmSouth incorrectly believed that: if it reported the transaction to the NASD, the bank did not need to file a SAR; if the matter involved civil litigation, the bank did not need to file a SAR; if it reported the matter to law enforcement by phone, the bank did not need to file a SAR; if the suspect were dead, the bank did not need to file a SAR (even though others might also be involved); and, last, if it did not suffer a loss, the bank did not need to file a SAR. This lack of understanding and training reflects poorly on senior management of the bank and its board of directors and makes it difficult for the bank to assert that it had a good BSA compliance process.

While, as stated above, the AmSouth case is controversial, the bank clearly did not have an adequate BSA and anti-money laundering program and did not have an adequate process for understanding the standards for filing SARs, or even for identifying and reviewing potentially suspicious activities. In addition, as described above, the case does not appear to have been based on the bank’s failure to file a solitary SAR. As the Assistant United States Attorney handling the case was quoted as saying: “bankers would be wrong to think the case was just about a failure to file reports. ‘If you read the documents carefully, there was a lot going on with this bank other than not filing one SAR... There are other charges that could have been brought against this bank.’”

167. Id.
168. Id. at 12-13; FinCEN Amsouth Assessment, supra note 147, at 6-8.
169. FinCEN Amsouth Assessment, supra note 147, at 6-8.
170. Id.
This understanding was reflected in comments made by Daniel P. Stipano, Deputy Chief Counsel of the Office of the Comptroller of the Currency:

Since the SARs system was introduced less than a decade ago, . . . it 'was never designed to be a gotcha game.' . . . Stipano said some of the recent scandals involving failures to file SARs could be considered 'misnomers' because they really involved much larger money laundering violations. . . . The convenient plea to cop to is a criminal violation of BSA. Criminal failure to file SARs is part of BSA, so it makes it look like . . . you're being dinged for not filing SARs, when in fact the problems were really much greater than that.172

As William Fox, Director of FinCEN, said with regard to the Riggs and AmSouth cases: "The danger is that the institutions misread what these actions are all about. It's so important to understand that in each of these cases, there were clearly systems failures, systems that were nonexistent or weak, as opposed to most institutions, we think, that have good systems in place."173

Consequently, it would appear that the sound message to take away from the AmSouth case, as well as the other cases detailed above, is that it is essential to have a culture within the bank that will ensure strong internal controls, a good BSA compliance program, an adequate system to investigate and report suspicious activity, an ability to monitor transactions and a willingness to respond to concerns and inquiries from officers and employees within the bank, as well as from outside sources, including law enforcement agencies.

V. CONCLUSION

The cases described above serve primarily to underscore the need for all banks to have a strong BSA compliance program. Failure to do so is obviously fraught with risk. While criminal liability for


173. Krebsbach, supra note 98, at 38.
banks is relatively rare,\textsuperscript{174} it has increased in recent years. In addition, there is the risk of administrative actions for BSA compliance failures that can involve the imposition of a cease and desist order,\textsuperscript{175} as well as the assessment of a large civil money penalty by the banking agency or by FinCEN.\textsuperscript{176}

In spite of these risks, though, it should be noted, as William Fox, Director of FinCEN, has said, “failures in compliance are by no means emblematic of the financial industry as a whole which functions well in complying with its anti-money laundering reporting requirements.”\textsuperscript{177} These words echo what he said with regard to the Riggs and AmSouth cases: “The danger is that the institutions misread what these actions are all about. It’s so important to understand that in each of these cases, there were clearly systems failures, systems that

\textsuperscript{174} See Cowden, \textit{supra} note 172, at 660. Lester M. Joseph, Principal Deputy Chief of the Department of Justice’s Asset Forfeiture and Money Laundering Section, has stated that there have been only four banks that have faced criminal action based on the failure to file SARs: Broadway National Bank, AmSouth Bank, Banco Popular and Delta National Bank. With the recent criminal plea by Riggs, the count is now five. \textit{Id.}

\textsuperscript{175} See 12 U.S.C. § 1818(s)(2000) which requires the imposition of a cease and desist order whenever a bank “has failed to establish and maintain the [BSA] procedures [required by each federal banking agency] or has failed to correct any problem with the procedures maintained by such depository institution which was previously reported to the depository institution by such agency” \textit{Id.} 12 U.S.C. § 1818(s)(3)(2000).

\textsuperscript{176} In the recent past, there have been three large civil money penalties cases other than the ones discussed above. Great Eastern Bank of Florida, Miami, Florida, was assessed $100,000 by FinCEN on Sept. 4, 2002, for failure to file SARs on six different customers who were engaging in large and suspicious back-to-back wire activity, depositing large amounts of cash followed by international wire activity and depositing a large volume of sequentially numbered money orders and travelers checks. \textit{See} Financial Crimes Enforcement Network Assessment of Civil Money Penalty, In the Matter of Great Eastern Bank of Florida, Financial Crimes Enforcement Network (Sept. 4, 2002), \textit{available at} http://www.fincen.gov/geassessfinal.pdf. Western Union Financial Services, Inc. was fined $8 million by the State of New York and an additional $3 million by FinCEN on March 6, 2003, for failure to aggregate multiple cash transactions among different Western Union agents, which resulted in a failure to file CTRs and SARs. \textit{See} Financial Crimes Enforcement Network Assessment of Civil Money Penalty and Undertakings, In the Matter of Western Union Financial Services, Inc., Financial Crimes Enforcement Network (Mar. 6, 2003), \textit{available at} http://www.fincen.gov/western_union_assessment.pdf. Korea Exchange Bank, New York, New York, was assessed a 1.1 million civil money penalty by FinCEN for failure to file 39 SARs involving $32 million in cash deposits that were wired out of the bank shortly after being deposited, for failure to file reports for ten months pursuant to the wire transfer rule involving transfers of $3,000 or more and failure to properly report 65 wire transfers just under the $3,000 reporting rules. \textit{See} Financial Crimes Enforcement Network Assessment of Civil Money Penalty, In the Matter of Korean Exchange Bank, Financial Crimes Enforcement Network (June 24, 2003), \textit{available at} http://www.fincen.gov/koreaexchangeassessment.pdf.

\textsuperscript{177} FinCEN Riggs Press Release, \textit{supra} note 32.
were nonexistent or weak, as opposed to most institutions, we think, that have good systems in place."\textsuperscript{178} As set forth in one article: "compliance often requires consideration of much detail, but with a bit of planning and foresight any bank can get it right."\textsuperscript{179}

The OCC has issued a guide for bankers entitled "Money Laundering: A Banker's Guide to Avoiding Problems."\textsuperscript{180} This booklet contains a lot of helpful information and detailed explanations, such as:

Comprehensive customer due diligence programs are banks' most effective weapons against being used unwittingly to launder money or to support terrorist financing. Knowing customers, including depositors and other users of bank services, requiring appropriate identification, and being alert to unusual or suspicious transactions can help deter and detect money laundering and terrorist financing schemes. Effective due diligence systems are also fundamental to help ensure compliance with suspicious activity reporting regulations.\textsuperscript{181}

An effective BSA compliance program includes controls

\textsuperscript{178} Krebsbach, supra note 98, at 38.

\textsuperscript{179} Mollie N. Sudhoff and Lucy H. Griffin, BSA confusion got you coming and going?, 96 A.B.A. BANKING JOURNAL, Nov. 1, 2004, at 74.


\textsuperscript{181} Money Laundering Guide, supra note 180, at 9.
and measures to identify and report suspicious transactions promptly. Financial institutions must employ appropriate customer due diligence to effectively evaluate transactions and conclude whether to file a suspicious activity report.\textsuperscript{182}

Bank anti-money laundering programs should be structured to address the controls needed based on the risks posed by the products and services offered, customers served, and geographies. The following are examples of high-risk products and services, customers, and geographic locations of which banks should be aware when developing a risk-based anti-money laundering program.\textsuperscript{183}

The Banker’s Guide provides the following examples:

- **High-Risk Products and Services**
  - Wire transfers / International correspondent banking
  - Private banking relationships
  - Electronic banking

- **High-Risk Customers**
  - Nonbank financial institutions, including Money Service Businesses
  - Non-governmental organizations (e.g., charitable organizations)
  - Offshore corporations, bearer share corporations, and banks located in tax and/or secrecy havens and jurisdictions designated as non-cooperative in the fight against money laundering
  - Cash-intensive businesses (convenience stores, parking garages, restaurants, retail stores)

- **High-Risk Geographic Locations**
  - Jurisdictions identified by intergovernmental organizations (e.g.,
Financial Action Task Force or FATF) as non-cooperative in the
fight against money laundering (commonly known as non-
cooperative countries and territories or NCCT)
• Countries or jurisdictions identified by the U.S. Department of
State’s annual International Narcotics Control Strategy Report
(INCSR) as being a “primary concern” for narcotics trafficking
and/or money laundering
• Geographies identified by OFAC
• Jurisdictions designated by the Secretary of the Treasury as
being of primary money laundering concern, as authorized by
§ 311 of the USA Patriot Act
• Jurisdictions identified by bank management. 184

The OCC Guide also lists various red flags that banks should be
aware of. 185 In creating its own “best practices” and BSA compliance
program, a bank should look at these factors and, moreover, concentrate
on the risk posed by its products, services and customers, ensure that it
understands and can manage those risks. The most important single
factor is the establishment of a strong culture by the board of directors
and senior management of the bank to create and adhere to an
appropriate and adequate anti-money laundering program. Banks
should recognize the increased attention being paid to anti-money
laundering enforcement by bank regulators, FinCEN, and federal
prosecutors. The risk of criminal prosecution, substantial civil money
penalties, and the loss of reputation are significant, as the cases detailed
above demonstrate, and banks should respond with renewed efforts to
develop and maintain adequate BSA programs.

184. Id. at 13-17.
185. Id. at 18-23.