

**UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK**

**IN THE MATTER OF
RIGGS BANK, N.A.**

No. 2004-01

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Secretary of the United States Department of the Treasury has delegated to the Director of the Financial Crimes Enforcement Network (“FinCEN”) the authority to determine whether a financial institution has violated the Bank Secrecy Act, 31 USC §§5311 et seq. and 31 CFR Part 103 thereunder (“BSA”), and what, if any, sanction is appropriate.

In order to resolve this matter, and only for that purpose, Riggs Bank N.A. (“Riggs”) has entered into a CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY (“CONSENT”) dated May 13, 2004, without admitting or denying FinCEN’s determinations described in Sections III and IV below, except as to jurisdiction in Section II below, which is admitted.

The CONSENT is incorporated into this ASSESSMENT OF CIVIL MONEY PENALTY (“ASSESSMENT”) by this reference.

II. JURISDICTION

Riggs is the principal subsidiary of Riggs National Corporation, a publicly traded bank holding company based in Washington, D.C. As of December 31, 2003, Riggs had assets of approximately \$6 billion, deposits of \$4.29 billion, and stockholders’ equity of \$427.2 million. Riggs is a “financial institution” and a “bank” within the meaning of 31 USC §5312(a)(2) and 31 CFR §103.11. The Office of the Comptroller of the Currency (the “OCC”) is Riggs’ primary federal supervisory agency and examines Riggs for BSA compliance.

III. FINDINGS

A. Summary of Violations

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 (“AML 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 business that would ensure appropriate reporting, implementing the procedures it did have, and responding to classic “red flags” of suspicious conduct. Riggs failed to correct the violations and implement an adequate BSA program in a timely manner. Consequently, on July 16, 2003, the OCC entered into a comprehensive Consent Order with Riggs to correct the deficiencies and referred the BSA violations to FinCEN for a determination of whether a civil penalty was warranted. Since then, however, additional violations occurred and the OCC is concurrently issuing a supplemental Consent Order requiring additional corrective actions.

B. Violations of the Anti-Money Laundering Program Requirements

FinCEN has determined that Riggs has been in violation of the AML program requirements of the BSA. As of April 24, 2002, the BSA has required banks to establish an AML program to guard against money laundering. A bank regulated by a Federal functional regulator is deemed to have satisfied the requirements of 31 USC §5318(h)(1) if it implements and maintains an AML program that complies with the regulation of its Federal functional regulator governing such programs. 31 CFR §103.120. Since January 27, 1987, the OCC has required each bank under its supervision to establish and maintain a BSA compliance program that, at a minimum: (a) provides for a system of internal controls to ensure ongoing compliance; (b) provides for independent testing for compliance conducted by bank personnel or an outside party; (c) designates an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (d) provides training for appropriate personnel. 12 CFR §21.21(c).

Riggs’ program contained serious deficiencies and was not in compliance with the BSA regulations. In January 2003, Riggs’ program was deficient in all four elements required by the AML program regulation. Some of the internal control and audit deficiencies continued after the OCC’s Consent Order was issued. These deficiencies are described in detail below.

1. Internal Controls

Riggs’ system of internal controls was inadequate to ensure ongoing compliance with the BSA across all business lines. 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. Indeed, Riggs’ internal controls proved insufficient to detect and monitor risk, or to alert the bank to the need to take preventive or corrective action when the risk materialized.

Riggs did not implement an effective system to identify and assess the BSA/AML risk present throughout the institution. The risk matrices used in some of Riggs’ divisions all contained similar criteria, rather than being tailored to the particular lines of business on a risk-graded basis, which weakened their effectiveness. As a result, management was unable to define and analyze concentrations of risk in the accounts, customers, locations, and products of Riggs.

Riggs' customer due diligence program was weak and was not implemented in an effective or consistent manner. Certain areas of Riggs failed to acquire or to use the bank's account opening and customer activity information collection procedures. Further, customer due diligence information required by Riggs' policies and procedures was frequently missing. As a result, Riggs failed to identify a large number of accounts associated with the governments of two foreign countries. Moreover, Riggs' enhanced due diligence policies and procedures governing high-risk areas were weak or, in some cases, nonexistent. High-risk areas include high-risk transactions such as transactions payable upon proper identification ("PUPID"), high-risk customers such as check cashers and money remitters, and accounts involving high-risk international geographic locations including international private banking, embassy banking, politically exposed persons, and non-resident aliens. On two occasions, although Riggs' management said that the institution had discontinued PUPID transactions, Riggs allowed the transactions to continue.

Riggs also failed to implement adequate internal controls to ensure the identification of suspicious transactions and the timely filing of complete suspicious activity reports ("SARs") on reportable transactions. Riggs did not effectively use procedures and automated technology already in place to identify and review suspicious cash, monetary instruments, or wire activity. Riggs did not have procedures or internal controls to ensure that subpoenas and other government requests regarding accountholders were referred to the division responsible for investigating potential suspicious activity.

Finally, internal controls were lacking in Riggs' management of its largest banking relationship, which involved the accounts of a foreign government, its politically exposed persons, and the companies owned by such persons (described section III.C.3. below). There was insufficient staff and procedures to monitor the accounts and a lack of oversight over the account relationship manager and his staff. These problems continued even after numerous warning signs indicated that Riggs needed to take corrective action.

2. Independent Testing

Riggs did not implement an adequate system for independent testing of BSA compliance. The independent testing for compliance with the BSA was neither timely nor effective for the level of risk within Riggs. The internal audit could not verify that management's corrective action for identified deficiencies were effective or timely. In addition, the scope of the audit failed to include an evaluation of the areas of money laundering vulnerabilities, BSA compliance, or the suspicious activity reporting process.

3. Designation of Individual(s) to Coordinate and Monitor Compliance

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. In addition, the person(s) responsible for BSA compliance at Riggs failed to adequately monitor, identify, investigate, analyze, and report suspicious activity.

4. Training Appropriate Personnel

Training on monitoring and detecting suspicious activity was particularly weak at Riggs. For example, bank officer visits to customer business locations did not include assessments of BSA/AML risk factors. In addition, branch personnel most familiar with accounts held by money services businesses (“MSBs”) were unaware of the factors that typically are associated with suspicious activity and the new BSA registration requirements for MSBs.

In summary, Riggs failed to develop and maintain an effective BSA compliance program in violation of 12 CFR § 21.21(c) and, thus, failed to establish and implement an adequate AML program in violation of § 5318(h)(1) of the BSA and its implementing regulation, 31 CFR § 103.120. Riggs’ faulty AML program resulted in its violation of the suspicious activity and currency transactions reporting requirements of the BSA, as discussed below.

C. Violations of the SAR Requirements

FinCEN has determined that from 2000 through 2003, Riggs violated the SAR requirements of the BSA set forth in 31 USC §5318(g) and 31 CFR §103.18 by failing to file or by delinquently filing approximately 33 SARs. These 33 SARs represent at least \$98 million in suspicious transactions.¹

1. SAR Requirements

A bank must report any transaction involving or aggregating to at least \$5,000 that it “knows, suspects, or has reason to suspect” (i) involves funds derived from illegal activities or is conducted to disguise funds derived from illegal activities, (ii) is designed to evade the reporting or recordkeeping requirements of the BSA (e.g., structuring transactions to avoid currency transaction reporting) or (iii) “has no business or apparent lawful purpose or is 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

¹ These SARs report transactions and categories of transactions described below. Generally, Riggs’ SAR program suffered from a lack of timeliness. FinCEN’s review of SARs filed by Riggs from February 2000 through April 2004 disclosed an additional 61 SARs that were filed more than 60 days after the suspicious activity occurred.

after examining the available facts, including the background and possible purpose of the transaction.” 31 USC §5318(g) and 31 CFR §103.18.

The SAR regulation requires a bank to file SARs “to the extent and in the manner required by this section” by “completing” a SAR Form. 31 CFR §103.18(a). A bank must file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. 31 CFR §103.18(b)(3) and Instructions to SAR Form, TD F 90-22.47. If no suspect is identified on the date of the detection of the incident requiring the filing, a bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case is reporting to be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. When filing a SAR, a bank must provide a detailed description of why the transaction was unusual, irregular, or suspicious in the narrative section of the form. Part V, SAR Form, TD F 90-22.47. The form requires “a chronological and complete account” of the transaction. The form emphasizes that the narrative description “is critical” and that the care with which it is written “may determine whether or not the described conduct and its possible criminal nature are clearly understood” by law enforcement.

To comply with the SAR rule, a bank must be able to determine whether transactions are in fact reportable. Therefore, a bank is required to have in place systems to identify the kinds of transactions and accounts that may be a high risk for money laundering or that exhibit indicia of suspicious activity, considering the type of products and services it offers and the nature of its customers. Otherwise, a bank cannot assure that it is in fact reporting suspicious transactions as required by the BSA.² In this case, the record shows that Riggs had information about its customers and their transactions that caused it to “know, suspect, or have reason to suspect” that many transactions were reportable suspicious transactions. However, Riggs failed to report these transactions, delinquently reported them, and/or filed incomplete reports because Riggs’ procedures to identify, analyze, and report suspicious activity were either non-existent or not implemented. As a result, Riggs violated the SAR requirements of 31 USC §5318(g) and 31 CFR §103.18.

2. Basic Deficiencies in SAR Procedures and Filings

As noted above, subpoenas and other matters were not appropriately referred for investigation. As a result, Riggs failed to identify for review accounts in which suspicious activity might be occurring. The SARs that were eventually filed by Riggs reported activity that occurred two to three years before the date of filing.

Structuring, which is the breaking up of transactions for the purpose of evading the BSA reporting and recordkeeping requirements, is often indicative of underlying illegal activity. It is also unlawful under the BSA. See 31 USC §5324. Structuring is one of the most basic situations that an effective SAR program should be designed to detect and report.³ Riggs failed to discover that several customers had been structuring

² See Matter of Korea Exchange Bank, No. 2003-04 (June 24, 2003).

³ See Matter of Western Union, No. 2003-2 (March 6, 2003).

transactions. These instances included the regular structuring of cash deposits into the bank, as well as the structuring of money order purchases. Riggs belatedly filed SARs on these transactions. However, most of these SARs were deficient because the narrative descriptions of the transactions were sparse and conclusory. Rather than providing specific information on the type, timing, and amount of activity observed in each account, Riggs simply stated that there was an appearance of structuring. Riggs also failed to report the total dollar amount allegedly structured in each account. Such deficiencies make it difficult for law enforcement to evaluate whether the activity described in the SAR is worth pursuing.⁴

3. Embassy Banking/International Private Banking Relationships

Extensive and frequent suspicious cash, monetary instrument, and wire activity at Riggs occurred within the accounts held by the government of a foreign country, politically exposed persons of that country, and the companies owned by such persons, where very little monitoring of activity was performed by the bank. Within this relationship, there were a number of transactions that exhibited classic indicators of suspicious activity, or at a minimum lacked any reasonable business or economic purpose, but were never identified and reported. These transactions included:

- aggregate cash withdrawals from the accounts of the government, politically exposed persons, and government employees that totaled tens of million of dollars over a 2-year period, the majority of which were conducted through PUPID transactions;
- dozens of sequentially numbered international drafts drawn from a politically exposed person’s account on 3 dates over a 2-month period, totaling millions of dollars, and made payable to the account holder, which were returned to Riggs for crediting back to the account; and
- dozens of sequentially numbered cashier’s checks purchased from the same above-listed account on 3 different dates over a period of six months, totaling tens of millions of dollars, and made payable to the account holder, half of which were returned to Riggs for deposit back into the account.

Riggs also failed to identify, monitor, and report suspicious activity related to the accounts of another foreign government, its politically exposed persons, and the companies owned by such persons. This was among Riggs’ largest depository relationships; however, the relationship manager for these accounts had little or no supervision. Riggs failed to monitor the activity in these accounts, despite various indicators in early 2003 that should have alerted it to the high-risk nature of the relationship, including publication of a newspaper article alleging official corruption and Riggs’ receipt of a subpoena requiring documents regarding the relationship.⁵ Meanwhile, Riggs failed to implement controls or monitor the ongoing activity.

⁴ See Matter of Great Eastern Bank of Florida, No. 2002-02 (Sept. 4, 2002).

⁵ Guidance on applying scrutiny to situations of this type has been available for some time. See Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Corruption (January

As a result of these deficiencies, Riggs could not properly identify, evaluate, and report suspicious activity occurring in the relationship, including activity by its employee, the relationship manager. Riggs failed to discover that the relationship manager had signatory authority over two accounts within the relationship, received funds from a government account within the relationship, and failed to file SARs on a timely basis. Examples of the relationship manager's suspicious transactions with respect to this relationship include:

- alteration of a check from the account of a politically exposed person who is the relative of a government official; and
- over \$1 million in wire transfers from accounts owned by the government into the account of a private investment corporation owned by the relationship manager at another U.S. bank.

Riggs also failed to identify, evaluate, and report on suspicious activity occurring in the accounts owned by the government involving transactions by and for the benefit of politically exposed persons, including:

- cash deposits into the account of a private investment corporation owned by a politically exposed person who is a government official, totaling millions of dollars, over a 2-year period; and
- wire transfers, totaling hundreds of thousands of dollars, from a government account to the personal account of another government official who had signature authority over the government account.

D. Violations of the CTR Requirements

FinCEN has determined that Riggs violated the BSA currency transaction reporting requirements set forth at 31 CFR §103.27(d) by failing to provide accurate information or omitting information on numerous currency transaction reports (“CTRs”). Under the BSA, banks are required to file CTRs for transactions in currency greater than \$10,000 in a single day. 31 USC §5313 and 31 CFR §103.22. Banks are required to file CTRs in the form prescribed by the Secretary of the Treasury and provide all the information called for by the form. 31 CFR §103.27(d).

The CTRs filed by Riggs on two markets did not contain the accurate legal names of those businesses. Over a one-year period, Riggs filed 90 CTRs representing \$6 million for one market and 52 CTRs representing \$1.3 million for the other market. The businesses had been long-standing customers of Riggs before Riggs began filing CTRs with their accurate legal names.

Riggs' failure to collect, document, and verify customer and account information resulted in its failure to provide accurate information on 6 CTRs filed on a company

2001), which was jointly issued by the Departments of the Treasury and State, the OCC, the Federal Reserve, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision.

owned by a politically exposed person who is a foreign government official. In the CTRs, Riggs reported the company's line of business as the export of timber, although the entity was actually a private investment company holding the personal investments of a politically exposed person who is a foreign government official. Together, the 6 CTRs revealed \$11.5 million in cash deposited over 2 years.

E. Willful Nature of BSA Violations

FinCEN has determined that Riggs' violations of the BSA and its implementing regulations were willful. The conduct of a bank may be characterized as willful if it demonstrates a reckless disregard for its obligations under law or regulation. As an OCC-supervised bank, Riggs was aware of the AML program, SAR, and CTR requirements of the BSA and its implementing regulations. Riggs' failure to establish and implement a BSA/AML program adequate to meet its suspicious activity and currency transaction reporting requirements constitute systemic violations demonstrating a reckless disregard of its obligations under the BSA.

Riggs' willfulness is further demonstrated by its failure to correct identified deficiencies. The OCC deemed Riggs' BSA compliance systemically deficient in 2003 and thus entered into a Consent Order with Riggs on July 16, 2003. However, Riggs is not in full compliance with the OCC's July 2003 Consent Order. Riggs' failure to establish and implement an adequate BSA compliance program, followed by its failure to correct deficiencies identified by its primary Federal regulator, is a pattern of conduct indicative of willfulness.

IV. CIVIL MONEY PENALTY

FinCEN has determined that by failing (1) to establish and implement an adequate AML program, (2) to file timely, accurate, and complete SARs, and (3) to file accurate and complete CTRs as described in Section III, above, Riggs willfully violated the AML program, SAR, and CTR provisions of the BSA and a civil money penalty is due pursuant to 31 USC §5321 and 31 CFR §103.57(f). In light of the seriousness of the violations, their continuing and ongoing nature, the potential harm they pose to the public, and taking into account the financial resources of Riggs, FinCEN has determined that the appropriate penalty amount in this matter is \$25 million.

V. CONSENT TO ASSESSMENT

In order to resolve this matter, and only for that purpose, Riggs, without admitting or denying either the facts or determinations described in Sections III and IV above, except as to jurisdiction in Section II, which is admitted, consents to the assessment of a civil money penalty against it in the sum of \$25 million. This penalty assessment shall be concurrent with the \$25 million penalty assessed against Riggs by the OCC. The penalty assessment of FinCEN and the OCC referenced above shall be satisfied by one payment of \$25 million to the Department of the Treasury.

Riggs agrees to pay the amount of \$25 million upon the assessment of the civil money penalty. Such payment shall be:

- a. made by certified check, bank cashier's check, or bank money order or by wire;
- b. made payable to the United States Department of the Treasury;
- c. any check or money order or copy of the wire transfer must be hand-delivered or sent by overnight mail to Nicholas A. Procaccini, Assistant Director and Chief Financial Officer, FinCEN, 2070 Chain Bridge Road, Suite 200, Vienna, Virginia 22182; and
- d. submitted under a cover letter, which references the caption and file number in this matter.

Riggs recognizes and states that it entered into the CONSENT freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever were made by FinCEN or any employee, agent, or representative of FinCEN to induce Riggs to enter into the CONSENT, except for those specified in the CONSENT.

Riggs understands and agrees that the CONSENT embodies the entire agreement between Riggs and FinCEN relating to this enforcement matter only, as described in Section III above. Riggs further understands and agrees that there are no express or implied promises, representations, or agreements between Riggs and FinCEN other than those expressly set forth or referred to in the CONSENT and that nothing in the CONSENT or this ASSESSMENT is binding on any other agency of government, whether federal, state, or local.

VI. RELEASE

Riggs understands that its execution of the CONSENT and compliance with the terms of this ASSESSMENT and the CONSENT constitute a complete settlement of civil liability for reporting and recordkeeping violations of the BSA, and the regulations promulgated thereunder, which were identified by the OCC prior to the date hereof.

By: _____ //s// _____

William J. Fox, Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury

Date: _____ May 13, 2004 _____