

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

**IN THE MATTER OF
AMSOUTH BANK**

No. 2004-2

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 and its implementing regulations, 31 USC §§5311 *et seq.* and 31 CFR Part 103 thereunder, and what, if any, sanction is appropriate.

In order to resolve this matter, and only for that purpose, AmSouth Bank ("AmSouth") has entered into a CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY ("CONSENT") dated October 12, 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

AmSouth is a subsidiary of AmSouth Bancorporation, a publicly traded company. Both entities are based in Birmingham, Alabama. As of December 31, 2003, AmSouth Bancorporation had assets of approximately \$45.6 billion, deposits of \$30.4 billion, and stockholders' equity of \$3.2 billion. AmSouth is a "financial institution" and a "bank" within the meaning of 31 USC §5312(a)(2) and 31 CFR §103.11. The Board of Governors of the Federal Reserve System (the "Federal Reserve") is AmSouth's primary federal supervisory agency and examines AmSouth for Bank Secrecy Act compliance.

III. FINCEN'S DETERMINATIONS

A. Summary of Violations

FinCEN has determined 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 laundering 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. These systemic deficiencies in AmSouth's anti-money laundering program resulted in AmSouth's failure to timely file suspicious activity reports in circumstances where the Bank was aware of suspicious activity by its customers. FinCEN has concluded that these failures warrant a civil penalty, to be assessed concurrently with the civil penalty by the Federal Reserve. Concurrently with this CONSENT, the Federal Reserve is entering into a comprehensive Cease and Desist Order and Order of Assessment of a Civil Money Penalty with AmSouth requiring, in addition to payment of a civil penalty, corrective action to bring AmSouth into compliance with its Bank Secrecy Act obligations.

B. Violations of the Anti-Money Laundering Program Requirements

FinCEN has determined that, since April 24, 2002, AmSouth has been in violation of the anti-money laundering program requirements of the Bank Secrecy Act. Every bank was required to establish an anti-money laundering program by April 24, 2002, that guards against money laundering and terrorist financing and ensures compliance with the Bank Secrecy Act and its implementing regulations. 31 USC §5318(h)(1) and 31 CFR §103.120. A bank regulated by a federal functional regulator is deemed to have satisfied these requirements if it develops and maintains an anti-money laundering program that complies with the regulation of its federal functional regulator governing such programs. 31 CFR §103.120. The Federal Reserve requires each bank under its supervision to establish and maintain a Bank Secrecy Act compliance program that, at a minimum: (a) provides for a system of internal controls to ensure ongoing compliance; (b) designates an individual or individuals responsible for coordinating and monitoring day-to-day compliance; (c) provides training for appropriate personnel; and (d) provides for independent testing for compliance conducted by bank personnel or an outside party. 12 CFR §208.63.

During its June 2004 examination of the Bank, the Federal Reserve Bank of Atlanta identified deficiencies in AmSouth's anti-money laundering program. FinCEN has determined that AmSouth's program was materially deficient in three of the four required elements. Specifically, AmSouth's anti-money laundering program had deficient internal controls that lacked sufficient policies and procedures to guide and direct the activities of its employees, ineffectively used the automated systems in place to monitor for suspicious activity across the enterprise, and lacked adequate board and management

oversight. AmSouth's employee training was insufficient, with both management and staff lacking a clear understanding of their obligations and how to accomplish them. Finally, the independent audit function was inadequate. These deficiencies are described in further detail below.

1. Internal Controls

AmSouth failed to develop and implement adequate internal policies, procedures, and controls to ensure compliance with the Bank Secrecy Act and its implementing regulations. AmSouth did not meet its legal obligations to assess the Bank's risks or vulnerabilities to money laundering and terrorist financing and to tailor its policies, procedures, and controls accordingly. With the exception of its private banking line of business, AmSouth failed to conduct a risk assessment of its customer base to identify categories of high-risk customers, products, and geographic locations. The Bank lacked procedures to identify and monitor customers with cash-intensive activity to determine if the activity was suspicious. This due diligence failure resulted in the Bank's inability to tailor its due diligence procedures as appropriate to the varying degrees of risk posed by its customers, including the creation of enhanced due diligence procedures where warranted. It also prevented AmSouth from developing a method for monitoring the transactions of high-risk customers to determine if the actual activity was commensurate with expected activity and/or lacked any apparent business or legal purpose.

The Bank's anti-money laundering program lacked adequate internal controls and procedures to integrate information generated by a number of the Bank's units and departments that was necessary to enable the performance of appropriate due diligence, including compliance with Section 314(a) of the Patriot Act. Specifically, systems used at the Bank's branches for recording monetary instruments sold to non-accountholders were not fully integrated with the Bank's system for responding to requests sent by FinCEN under Section 314(a) of the Patriot Act. Despite the fact that such records must be maintained for Bank Secrecy Act compliance, the Bank could not determine whether the scope of its Section 314(a) searches was adequate for monetary instrument transactions.¹ Information maintained, and reports generated in various departments not directly involved in Bank Secrecy Act compliance, but which nevertheless inform the Bank of suspicious activity occurring within it (e.g., in litigation reports, fraud and loss prevention monitoring), were not regularly provided to Bank Secrecy Act compliance or Corporate Security personnel for appropriate action. For example, the Legal Department had no system in place to alert Bank Secrecy Act compliance personnel to subpoenas and information requests it received from law enforcement. In certain other cases, it did not provide information to the Bank Secrecy Act compliance or Corporate Security personnel about suspicious activity obtained through litigation activity and reports generated from it, which was used only to monitor and manage litigated cases. Many of the departments within AmSouth lacked adequate procedures and guidance regarding the delivery of information to appropriate personnel for suspicious activity determinations.

¹ This issue will be resolved and addressed in the course of the remedial actions by the Bank.

AmSouth failed to develop and implement policies, procedures, and internal controls adequate to ensure the referral, investigation, and reporting of suspicious transactions. In fact, AmSouth's policies and procedures lacked meaningful information on what constitutes a reportable event or the procedures to be followed in investigating and reporting suspicious transactions. Written procedures establishing criteria for, and directing employee decisions on, when to administratively close a referral or conduct an investigation and when to file a SAR were inadequate.

Finally, reporting to management for the purposes of monitoring and oversight of compliance activities was materially deficient. AmSouth lacked written procedures for the preparation of reports to senior management and the security director. Further, the reporting that did exist focused heavily on loss detection and prevention, to the detriment of Bank Secrecy Act compliance. Without adequate reporting, board and senior management committees responsible for overseeing some or all of the suspicious activity identification and reporting process could not be effective.

2. Training Appropriate Personnel

AmSouth management and staff lacked sufficient understanding of their Bank Secrecy Act compliance obligations in large part because of an inadequate training program. Before February 2004, AmSouth did not provide bank-wide training for detecting and reporting fraud and other forms of suspicious activity for employees. Suspicious activity reports were not filed because the business units were never instructed on what activity warrants reporting. Many employees did not understand their obligations. In fact, some personnel operated under the misapprehension that suspicious activity reports were not required to be filed unless there was a loss to the Bank, leading to failures in reporting that are discussed infra. Employees lacked sufficient knowledge and experience to detect and report suspicious activity.

3. Independent Testing for Compliance

AmSouth's independent testing for compliance with the Bank Secrecy Act and its implementing regulations was materially inadequate. AmSouth conducted its first ever enterprise-wide internal audit of Bank Secrecy Act compliance in 2003. However, the scope of AmSouth's review of suspicious activity identification, investigation, and filing procedures in the 2003 internal audit was inadequate and limited to a "reasonableness and completeness" check of suspicious activity reports that were actually filed. As a result, the audit did not review detection and monitoring reports, sample and test potentially suspicious accounts, or render an opinion, general or otherwise, on the overall adequacy of AmSouth's anti-money laundering program with respect to detecting, monitoring and reporting suspicious activity. The internal audit did not evaluate monitoring parameters to determine if they were appropriate or effective. The auditors did not confirm whether all accounts reflected on the monitoring reports received by compliance personnel were actually analyzed and resulted in either suspicious activity report filings or adequate notations of the reasons that the activity did not merit a suspicious activity report. No

accounts were independently sampled or tested for identification of suspicious activity. The audit thus was incapable of determining the adequacy of the procedures for monitoring, detecting, and reporting suspicious activity. Management's review of, and quality assurance over, the audit work performed, the findings documented, and the conclusions rendered were inadequate.

In summary, AmSouth failed to develop and maintain a Bank Secrecy Act compliance program appropriate for the size and complexity of its business in violation of 12 CFR §208.63 and, thus, failed to establish and implement an adequate anti-money laundering program in violation of §5318(h)(1) of the Bank Secrecy Act and its implementing regulation, 31 CFR §103.120. AmSouth's inadequate anti-money laundering program resulted in violations of the suspicious activity reporting requirements of the Bank Secrecy Act, as discussed below.

C. Violations of the Suspicious Activity Reporting Requirements

FinCEN has determined that AmSouth violated the suspicious activity reporting requirements of the Bank Secrecy Act and its implementing regulations set forth in 31 USC §5318(g) and 31 CFR §103.18. Because of AmSouth's inability to identify or monitor high-risk customers or transactions effectively, the Federal Reserve's June 2004 examination could not identify all transactions meriting the filing of a suspicious activity report. The Cease and Desist Order that AmSouth is entering into with the Federal Reserve simultaneously with this CONSENT will require AmSouth to continue its implementation of procedures to identify such circumstances and make the appropriate filings. However, FinCEN has identified examples of significant instances of suspicious activity known to the Bank, on which suspicious activity reports should have been, but were not filed, which are discussed below.

1. Suspicious Activity Reporting 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 Bank Secrecy Act (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 after examining the available facts, including the background and possible purpose of the transaction." 31 USC §5318(g) and 31 CFR §103.18. A bank must file a report no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing. 31 CFR §103.18(b) (3) and Instructions to Suspicious Activity Report 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 report 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.

In cases requiring immediate attention, a bank should notify law enforcement of the activity by telephone, but such notification does not relieve the bank of its obligation to file a suspicious activity report.

To comply with these rules, 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 of 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 Bank Secrecy Act. In this case, the record shows that AmSouth had information about its customers and their transactions that caused it to “know, suspect, or have reason to suspect” that certain transactions were reportable suspicious transactions. However, AmSouth failed to report these transactions or delinquent reported them because its procedures to identify, analyze, and report suspicious activity were inadequate. As a result, AmSouth violated 31 USC §5318(g) and 31 CFR §103.18.

2. Basic Deficiencies in Suspicious Activity Reporting Procedures and Filings

As a result of the defects in its anti-money laundering program described above, AmSouth regularly failed to identify for review accounts in which suspicious activity might be occurring. Even when personnel at the various business units had knowledge of suspicious activity in certain accounts, the Bank’s lack of training and/or referral procedures often prevented this information from being brought to the attention of the persons responsible for suspicious activity reporting. In some instances, Bank personnel incorrectly believed that reporting was not required because there was no loss to AmSouth. In other instances, certain Bank personnel would not file suspicious activity reports on activity that had been telephonically reported to law enforcement.² The lack of management oversight and review of the program exacerbated these problems.

3. Examples of AmSouth’s Reporting Violations

AmSouth failed to timely file suspicious activity reports regarding the following objectively suspicious activity by its customers:

- The perpetrators of a fraudulent investment scheme maintained accounts at AmSouth to handle funds contributed by individual investors. AmSouth did not perform adequate due diligence on the perpetrators, which could have revealed financial and prior regulatory problems. Further, AmSouth ignored red flags, including concerns communicated to Bank management by several employees at various AmSouth branches indicating the accounts were being used in furtherance

² Telephonic notice has never been permitted as a substitute for filing a suspicious activity report because all of the information required to be in a report must be available to all appropriate local, state, and federal law enforcement users that might be investigating related crimes or patterns of criminal activity.

of a Ponzi scheme. Despite such warnings, AmSouth failed to file a suspicious activity report until two years after it knew or should have known about the suspicious nature of the activity and millions had been deposited and then withdrawn from related accounts at the Bank. The perpetrators ultimately were convicted of money laundering and money laundering conspiracy.

- The Chief Financial Officer of an AmSouth corporate customer embezzled several million dollars from the corporation over three years using forged and improperly authorized checks. Although AmSouth employees noticed that the Chief Financial Officer was conducting a number of highly unusual transactions, the Bank did not file a suspicious activity report because it suffered no loss.
- A municipal official contacted the manager of a local AmSouth branch regarding the suspected misappropriation by another municipal official of approximately \$450,000 through the fraudulent endorsement of a number of city checks. Shortly thereafter, the responsible party acknowledged the misappropriation in a suicide note. Nonetheless, AmSouth did not file a suspicious activity report because the suspect was dead. Another municipal employee was eventually indicted for his role in the fraud.
- Another matter involved an employee of AmSouth's broker-dealer who allegedly committed fraud in clients' accounts by, among other things, forging customer signatures on numerous documents. The broker-dealer reported this employee's misconduct to the National Association of Securities Dealers ("NASD"). The broker-dealer also had a duty to report what it knew to be suspicious activity by its own employee to FinCEN, and it failed to do so. AmSouth now acknowledges that a SAR should have been filed in this matter, and recently filed a SAR.
- An employee of a car dealership formed his own corporation and then opened an account at AmSouth under the name of the corporation "dba" (doing business as) the name of the car dealership. Over a year, the employee deposited several hundred thousand dollars worth of checks made payable to his employer into the AmSouth account. The employer ultimately sued AmSouth concerning these transactions. AmSouth handled the litigation without conducting a review to determine whether a SAR should be filed.
- An individual operated a fraudulent multi-million dollar trading operation for five years before being arrested. More than \$20 million in assets from investors in the program were frozen in various banks, including AmSouth. AmSouth received Securities and Exchange Commission and grand jury subpoenas seeking information on the matter. Months after the individual pleaded guilty to felony charges of securities fraud, money laundering and wire fraud, AmSouth closed the last of his accounts without ever having filed a suspicious activity report.

- A corporate customer deposited into its AmSouth account an official check for \$220,000 drawn on another U.S. bank. Six days later, the customer initiated a wire transfer of \$190,000 from its AmSouth account to a bank in a foreign country. All but \$30,000 of the wired funds were then withdrawn from the foreign bank. Nine days after its deposit, the check was returned unprocessed to AmSouth because the amount had been altered. Although AmSouth notified local law enforcement of the incident, and fully cooperated with the government investigation, it did not file a suspicious activity report.
- A bank cashier at another bank embezzled money from his employer by wiring funds from an account maintained by his employer to deposit accounts at AmSouth held in his or his wife's name. The bank cashier then invested these funds in investment accounts at AmSouth's broker-dealer subsidiary. The employer contacted AmSouth about the bank cashier's accounts. Although AmSouth notified federal law enforcement of the incident, it never filed a suspicious activity report.

In addition, the Federal Reserve's June 2004 examination disclosed that AmSouth had not filed suspicious activity reports on a number of instances of check kiting activity involving possible losses above \$5,000, which appeared on an AmSouth internal report. In response to the examination, AmSouth has now filed suspicious activity reports on several of the matters identified by the Federal Reserve. Various cases involving fraudulent activity by customers of the bankcard business unit, and matters identified by the fraud prevention unit, also were not reported.

D. Willful Nature of BSA Violations

The conduct of a bank may be characterized as willful if it demonstrates a reckless disregard for its obligations under law or regulation. As a bank supervised by the Federal Reserve, AmSouth was aware of the anti-money laundering program and suspicious activity reporting requirements of the Bank Secrecy Act and its implementing regulations. AmSouth had material deficiencies in the basic elements of its anti-money laundering program, which led to violations of the suspicious activity reporting requirements in a number of significant instances. These violations were systemic and serious. FinCEN has determined that AmSouth's violations of the Bank Secrecy Act and its implementing regulations were willful.

IV. CIVIL MONEY PENALTY

FinCEN has determined that by failing to establish and implement an adequate anti-money laundering program and to file and file timely suspicious activity reports as described in Section III, above, the AmSouth willfully violated the anti-money laundering program and suspicious activity reporting provisions of the Bank Secrecy Act and its implementing regulations a civil money penalty is due pursuant to 31 USC §5321 and 31 CFR §103.57(f).

V. CONSENT TO ASSESSMENT

In order to resolve this matter, and only for that purpose, AmSouth, 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 \$10 million. This penalty assessment shall be concurrent with the \$10 million penalty assessed against AmSouth by the Federal Reserve. The penalty assessment of FinCEN and the Federal Reserve referenced above shall be satisfied by one payment of \$10 million to the Department of the Treasury.

AmSouth agrees to pay the amount of \$10 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. evidenced by a check or money order or copy of the wire transfer, hand-delivered or sent by overnight mail to Nicholas A. Procaccini, Acting Associate Director, Administration and Communications, 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.

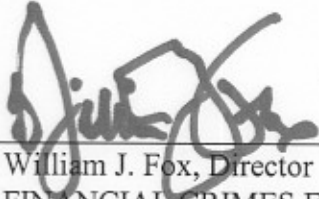
AmSouth recognizes and states that it enters into the CONSENT freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce AmSouth to enter into the CONSENT, except for those specified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

AmSouth understands and agrees that the CONSENT embodies the entire agreement between AmSouth and FinCEN relating to this enforcement matter only, as described in Section III above. AmSouth further understands and agrees that there are no express or implied promises, representations, or agreements between AmSouth 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

AmSouth 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 Bank Secrecy Act, and the

regulations promulgated thereunder, which were identified by the Federal Reserve prior to the date hereof.

By: 

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

Date: OCT 12 2004