FINANCIAL INDUSTRY REGULATORY AUTHORITY
OFFICE OF HEARING OFFICERS

DEPARTMENT OF ENFORCEMENT, Complainant, v. STERNE, AGEE & LEACH, INC. (CRD No. 791), Respondent.	Disciplinary Proceeding No. E052005007501 Hearing Officer – LBB **HEARING PANEL DECISION** March 5, 2010

Respondent violated NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41, by failing to implement an adequate anti-money laundering program for 2006 – 2007. For these violations, Respondent is fined $40,000.

Appearances

For the Department of Enforcement, Laura Leigh Blackston, Senior Regional Counsel, New Orleans, Louisiana, and Karen E. Whitaker, Senior Regional Counsel, Dallas, Texas.

For Respondent, Gerald J. Russello, Esq., New York, New York, and Paul M. Tyrrell, Esq., Boston, Massachusetts.

DECISION[1]

The Complaint in this disciplinary proceeding was filed on August 5, 2008, charging Respondent Sterne, Agee & Leach, Inc. ("Respondent" or "Sterne Agee") with violating NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41, by failing to develop and implement an adequate anti-money laundering ("AML") program from April 24, 2002, through July 11, 2005, due to certain alleged broad deficiencies in the program. In addition, the Complaint alleges that

[1] This Decision has been redacted to remove or obscure references to information that might be deemed non-public under the anti-money laundering laws.

there were several specific deficiencies in Respondent's AML program from July 1, 2006, through April 20, 2007.[2]

For April 2002 through July 2005, the focus of the Department of Enforcement's ("Enforcement") case was its contention that Respondent could not adequately detect activities that required investigation or reporting under the AML laws because Respondent's AML system was insufficiently automated. The Complaint also alleges that during that period, Respondent's AML procedures provided insufficient guidance to its operational personnel concerning the detection of potential money laundering and the procedures for escalating potential money laundering activities for review by the firm. In addition, the Complaint alleges that Respondent's AML training program was inadequate. The Hearing Panel finds that Respondent's AML procedures from April 2002 through July 2005 were reasonably designed to achieve and monitor Respondent's compliance with the AML laws, as required by Conduct Rule 3011.

For July 2006 through April 2007, the Complaint alleges that there were six specific deficiencies in the design and implementation of Respondent's AML program: (1) inadequate procedures for review of physical securities certificates; (2) inadequate procedures for monitoring journal transfers; (3) inadequate procedures for identifying direct foreign financial institution accounts; (4) failure to have written procedures to comply with the enhanced due diligence requirements of Section 312 of the USA PATRIOT Act; (5) failure to identify certain accounts as accounts for foreign banks, to obtain certifications for those foreign banks, and to

---

[2] As of July 30, 2007, NASD consolidated with the member regulation and enforcement functions of NYSE Regulation and began operating under a new corporate name, the Financial Industry Regulatory Authority (FINRA). References in this decision to FINRA include, where appropriate, NASD. Following consolidation, FINRA began developing a new FINRA Consolidated Rulebook. The first phase of the new consolidated rules became effective on December 15, 2008, including certain conduct rules and procedural rules. *See* Regulatory Notice 08-57 (Oct. 2008). This decision refers to and relies on the NASD Conduct Rules that were in effect at the time of Respondent's alleged misconduct. In addition, because the Complaint was filed before December 15, 2008, the NASD Procedural Rules were applied in this disciplinary proceeding.

send the notifications required by Section 311 of the USA PATRIOT Act to those banks; and (6) failure to implement customer identification procedures for delivery versus payment accounts. The Hearing Panel finds that Respondent violated Conduct Rules 3011 and 2110, and MSRB Rule G-41, because the AML program for this period had certain of the deficiencies charged in the Complaint, as set forth below.

A hearing was held in New Orleans from April 6 through April 9, 2009, before a Hearing Panel consisting of one current member of the District 5 Committee, one former member of the District 5 Committee, and a Hearing Officer. Three FINRA examiners, three current and former employees of Sterne Agee, and an expert witness for each party testified at the hearing.

I. RESPONDENT

Sterne Agee is a regional clearing firm, with its main office in Birmingham, Alabama. In addition to functioning as a clearing firm, Respondent had other lines of business, transacted through affiliates, including affiliates that were introducing firms. Stip. 1; Tr. 554, 632.[3] During all relevant periods in the Complaint, Respondent was a registered broker-dealer with the United States Securities and Exchange Commission ("SEC"). Respondent has been a member of FINRA since October 16, 1936. Stip. 1.

In 2005 and 2006, Respondent had about 400 employees, of whom about half were registered representatives. Tr. 703. The firm cleared for about 80 introducing firms, engaging in about 75,000 transactions per month. Tr. 555.

---

[3] References to the exhibits provided by Enforcement are designated as "CX-___." References to the exhibits provided by Respondent are designated as "RX-___." References to the stipulations by the parties are identified as "Stip. __." References to the hearing transcript are designated as "Tr. ___."

II. Overview of the Bank Secrecy Act and Implementing Rules and Regulations

A. The USA PATRIOT Act and NASD Conduct Rule 3011

The Bank Secrecy Act ("BSA"), initially adopted in 1970, established the framework for anti-money laundering obligations imposed on financial institutions. The Department of the Treasury ("Treasury") delegated the authority to administer the BSA to the Financial Crimes Enforcement Network ("FinCEN").[4] The BSA was amended in 2001 by Title III of the USA PATRIOT Act (the "Patriot Act").[5] Section 352 of the Patriot Act requires broker-dealers to establish AML programs, which must include written internal policies, procedures, and controls, the designation of a responsible compliance officer, ongoing training programs, and an independent audit to test the AML program.

In April 2002, FINRA issued Notice to Members ("NTM") 02-21, a Special Notice to Members on the new AML requirements for broker-dealers. NTM 02-21 provided guidance to assist members in developing AML compliance programs that fit their business models and needs. The NTM emphasized each firm's duty to detect red flags that might be signs of money laundering and, if any were detected, to "perform additional due diligence before proceeding with the transaction."[6]

On April 24, 2002, FINRA adopted NASD Conduct Rule 3011,[7] which requires each member firm to "develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the member's compliance with the requirements of the [BSA],

---

[4] *See* Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions, 67 Fed. Reg. 44048, at 44053 (July 1, 2002).

[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[6] NTM 02-21, at 10.

[7] Order Approving Proposed Rule Changes Relating to Anti-Money Laundering Compliance Programs, 67 Fed. Reg. 20854 (Apr. 26, 2002).

and the implementing regulations promulgated thereunder by [the U.S. Department of the Treasury]."[8]

B. Suspicious Activity Reporting

NASD Conduct Rule 3011(a) requires each member to establish and implement policies and procedures "that can be reasonably expected to detect and cause the reporting of" suspicious activity and transactions.

Section 356 of Title III of the Patriot Act required Treasury to issue final regulations requiring broker-dealers to report suspicious transactions under 31 U.S.C. §5318(g). FinCEN amended its BSA regulations on July 1, 2002, implementing the Patriot Act requirements for broker-dealers. The regulations provide that, with respect to any transaction after December 30, 2002, "[e]very broker or dealer in securities within the United States … shall file with FinCEN … a report of any suspicious transaction relevant to a possible violation of law or regulation."[9] Section (a)(2) of the regulations requires broker-dealers to report to FinCEN any transaction that, alone or in the aggregate, involves at least $5,000 in funds or other assets, if the broker-dealer knows, suspects, or has reason to suspect that: (1) the transaction involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; (2) the transaction is designed, whether through structuring or other means, to evade the requirements of the BSA; (3) the transaction appears to serve no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts; or (4) the transaction involves use of the broker-

[8] MSRB Rule G-41 requires brokers, dealers, and municipal dealers to establish an AML program that is reasonably designed to achieve and monitor ongoing compliance with the requirements of the BSA. Compliance with NASD Rule 3011 is deemed to be sufficient to meet the requirements of MSRB Rule G-41. References in this decision to the requirements of NASD Rule 3011 are intended to include the requirements of MSRB Rule G-41.

[9] 31 C.F.R. § 103.19(a)(1).

dealer to facilitate criminal activity.[10] A broker or dealer in securities must file a suspicious activity report no later than 30 calendar days after the date of initial detection of a reportable transaction.[11]

In August 2002, FINRA issued NTM 02-47, which set forth the provisions of the final AML rule for suspicious transaction reporting promulgated by FinCEN for the securities industry. NTM 02-47 advised broker-dealers of their duty to file a Suspicious Activity Report ("SAR") form for certain suspicious transactions occurring after December 30, 2002, in accordance with the regulations issued by FinCEN. FINRA noted that the final rule requires that broker-dealers determine whether activities surrounding certain transactions raise suspicions of no business or apparent lawful purpose by looking for red flags such as those enumerated in NTM 02-21.

C. Customer Identification

Section 326 of the Patriot Act required Treasury and the SEC to issue a rule requiring broker-dealers to implement reasonable procedures to: (1) verify the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintain records of the information used to verify the person's identity; and (3) determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency. On April 30, 2003, FinCEN and the SEC jointly issued a final rule to implement Section 326 of the Patriot Act. The final rule required each broker-dealer to establish a written customer identification program to verify the identity of each customer who opens an account.[12]

---

[10] *See* NTM 02-47 (Aug. 2002).

[11] 31 C.F.R. § 103.19(b)(3).

[12] Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25113 (May 9, 2003); NTM 03-34.

III. RESPONDENT'S AML PROGRAM WAS REASONABLE, AND COMPLIED WITH NASD CONDUCT RULE 3011, IN 2002 THROUGH 2005

The Complaint alleges that from April 24, 2002, when broker-dealers were first required to implement AML programs, until July 11, 2005, Respondent's AML program could not reasonably assure compliance with the requirements of the BSA and NASD Conduct Rule 3011(a) because Respondent "had no meaningful way to monitor and potentially identify suspicious activity for its introduced accounts."[13] Thus, for this period, the Complaint alleges a violation only for Respondent's clearing business.[14]

The Complaint characterized Respondent's system for detecting suspicious activity in introduced accounts as a "largely manual system." Enforcement took the position at the hearing that a manual system could not have adequately detected suspicious activity, and presented expert testimony that a substantially more automated system was required. In addition, the Complaint alleges that Respondent's procedures provided insufficient guidance to its employees on how to identify and review transactions for AML issues, and how to "escalate" the review when AML issues were identified. The Complaint also charges that Respondent's AML training was inadequate.

Sterne Agee made substantial efforts to design and implement an effective AML program. As discussed below, the Hearing Panel finds that Sterne Agee's AML program for April 2002 through July 2005 could "be reasonably expected to detect and cause the reporting of" suspicious activity and transactions. Enforcement failed to show that it was unreasonable to rely

[13] Although the Complaint alleges that the deficiencies were present starting April 24, 2002, the first day that AML procedures were required, there was very little evidence offered concerning the period prior to 2003. The review period for the examination that led to the allegations in the Complaint concerning 2002 – 2005 was September 20, 2003, through July 8, 2005, and most of the evidence related to the period reviewed by the examiner. Tr. 34.

[14] FINRA has emphasized that "both introducing brokers and clearing brokers have responsibilities under the Money Laundering Abatement Act…. In order to detect suspicious activity, it is imperative that introducing and clearing brokers work together to achieve compliance with the Money Laundering Abatement Act." NTM 02-21, at 15.

on a system with a substantial manual component to detect potential money laundering activity during that period. Enforcement also failed to show that Respondent's AML procedures provided insufficient guidance to Sterne Agee's staff in identification and review of transactions for AML issues, or that the training was inadequate to give its staff sufficient guidance on how to review transactions.

A. Organization of Respondent's AML Program

Respondent's AML program was well organized. The firm had a full-time AML compliance officer. Operations personnel were responsible for the initial detection of AML issues in their respective areas of responsibility, under the supervision of management within the Operations Department.

1. AML Compliance Officer

Conduct Rule 3011(d) and Section 352 of the Patriot Act require broker-dealers to designate an AML compliance officer. Timothy Vardaman, a vice president and the risk division manager, took on the added responsibility as Sterne Agee's AML compliance officer in late 2001. In April 2003, he began to turn that responsibility over to Michael Keener, who had previously been the firm's regulatory reporting manager, responsible for a variety of reports such as FOCUS reports. Tr. 225, 449 - 450, 453, 553; CX-13 at 7; CX-55. When Keener became the AML compliance officer in July 2003, it became a full-time position. Tr. 552, 702.

2. Monitoring for AML Issues by Operational Personnel

Respondent's system for detecting possible suspicious activity included manual reviews by employees in the Central Cashiering Department to monitor all deposit activity; in the Margin Department to monitor wire activity, journal activity, and fund disbursements; in the Cash Management Department to monitor incoming wires; and in the New Accounts Department to monitor foreign accounts and new accounts. Stip. 8; CX-1 at 15; Tr. 562.

The Margin Department, Central Cashiering Department, and New Accounts Department were within the Risk Division, which was part of the Operations Department. The Operations Department was supervised by the chief operations officer. The risk division manager reported to the chief operations officer, and managers of the departments within the Risk Division reported to the risk division manager. Each of those departments had a manager with several years of experience with Sterne Agee. Tr. 457, 472 – 473. In some instances, the departments had supervisors under the managers. Each department had a clerical staff reporting to the supervisor or manager. Tr. 457.

B. Respondent's Written AML Procedures

Respondent developed and implemented written AML policies and procedures ("AML Manual") by the April 24, 2002, deadline established under the BSA. Stip. 2. The AML Manual was based on FINRA's AML Money-Laundering Template for Small Firms, with some modifications.[15] Respondent updated its policies and procedures several times over the years as the regulators issued additional AML guidance. Tr. 626. The written procedures included a list of about 25 red flags that were identified as indicia of possible money-laundering activity in accounts.[16] The procedures required Respondent's employees to report red flags, or any other suspicious or unusual account activity, to the AML compliance officer immediately upon detection. CX-1 at 13, 15; CX-26 at 17. The Hearing Panel finds that the descriptions of the red

---

[15] Using the Small Firm Template does not ensure that a firm's AML program complies with the requirements of Rule 3011. The Small Firm Template states, "This template is provided to small firms to assist them in fulfilling their responsibilities to establish an Anti-Money Laundering Program as required by the USA PATRIOT Act of 2001 and NASD Rule 3011. … [F]ollowing this template does not guarantee compliance with those requirements or create a safe harbor from regulatory responsibility.… The obligation to develop an AML plan is not a 'one-size-fits-all' requirement, and you must tailor your plan to fit your particular firm's situation." The Hearing Panel does not rely on the use of the Template as a basis for its conclusions with respect to whether Respondent violated Rule 3011.

[16] The red flags were based on the list of red flags in the Small Firm Template. Tr. 565, 639; CX-1; CX-26; CX-44; CX-45. A similar list of red flags was included in guidance issued by the Securities Industry Association and FINRA. *SIA*, *Preliminary Guidance for Deterring Money Laundering Activity* (Feb. 2002), at 12 – 13; NTM 02-21, at 10 – 11.

flags were sufficiently specific to enable the Operations Department personnel to identify account activity that raised red flags.

C. Monitoring and Detection of Suspicious Activity

1. Automation of Account Information and AML Monitoring at Sterne Agee

Enforcement contends that Respondent's AML procedures were deficient because Respondent relied on a largely manual system for detection of suspicious activity, and therefore could not adequately detect patterns of suspicious activity and links among accounts. Respondent described its procedures in its 2003 AML Manual as follows: "[Sterne Agee] will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as 'non-cooperative' are involved, or any of the 'red flags' identified in 7b below." CX-1 at 12.

Respondent's system was actually a mix of manual and automated processes. Respondent used, and still uses, software known as BETA to record all activity in client accounts. Respondent kept track of money and stocks coming into or going out of accounts on the BETA system. Tr. 452, 461, 482. The BETA system was also used for new account information. Tr. 577. As discussed below, BETA produced a variety of reports that were used in AML monitoring.

In 2003, Respondent began the process of using AML monitoring software from Protegent. The software was implemented in 2004. The vendor had told Respondent before the system was implemented that the Protegent software would monitor both introduced accounts and accounts from Respondent's affiliates. After using the software for about four months, Respondent realized that the software was monitoring transactions for accounts introduced by

Respondent's affiliates, but not for accounts introduced by Respondent's clearing clients. Tr. 583 – 584, 650 – 651. Accordingly, Respondent stopped using the software in mid-2004, and began creating its own reports. Tr. 650 – 651. When Respondent stopped using the software, the AML compliance officer conducted a retrospective review, examining the year-to-date data, covering about five months of clearing transactions, to identify suspicious activity, and provided his findings or analysis to the Ad Hoc Credit Committee.[17] CX-22; Tr. 583 – 586.

When the Protegent system did not meet Respondent's needs for software to monitor its clearing business, Respondent increased its use of software known as "BETA Access" for AML monitoring. Tr. 578, 583 – 585, 731.[18] BETA Access allowed Respondent to customize reports and gather a variety of types of information. Using BETA Access, Respondent could query the BETA database and show, for example, all trades, or all positions, and link data together. Respondent could then create a variety of tables and analysis tools, and compare information. Tr. 577 – 578, 585, 728. The AML compliance officer identified a long list of reports that he currently creates using BETA Access that look at a broad variety of account data in different ways. However, AML monitoring has been an evolving process, and it is unclear when Respondent first began using each of the various reports. Tr. 708 – 712.[19]

---

[17] The Ad Hoc Credit Committee, a committee of senior managers, was responsible for managing Respondent's risk. Tr. 585.

[18] Although the relationship between the BETA software and BETA Access was not explained at the hearing, the overall description of how the two programs work suggests that BETA Access was an enhancement or supplement to the basic BETA software, and that both were provided by a vendor that was named BETA.

[19] The AML compliance officer testified that he began to implement and use BETA Access in 2004, but that the system began to generate information in 2005. Tr. 578, 583 – 585. An independent audit of Respondent's AML program in 2003 refers to the ability to create various reports using BETA Access, suggesting that BETA Access had been implemented at that time, although it is not clear how it was used. *See* CX-13 at 13. Respondent clearly began to use it by June 2004, when the retrospective analysis was done and provided to the Ad Hoc Credit Committee after the discovery that the Protegent software was not monitoring Respondent's clearing business. CX-22.

Respondent did not look at fully-automated systems in 2003 through 2005 because the AML compliance officer was told by firms that were using AML monitoring software that they were unhappy with their systems, and BETA Access had some capabilities that AML software lacked. Tr. 731 – 734.

2. Customer Identification

Respondent implemented a customer identification program by the October 1, 2003, deadline established by Treasury and the SEC. Stip. 2. The New Accounts Department became involved in AML compliance when the customer identification program was implemented. CX-52 at 3. The customer identification program was outlined in the firm's AML Manual. CX-1; CX-26. Respondent's customer identification program required the firm to collect a variety of identifying information for each customer when opening new accounts. CX-1; CX-26. The New Accounts Department examined the new account documents to look for obvious fraud and forgery, and generally to look for signs of suspicious activity in new account items. Tr. 562, 639; CX-1 at 12; CX-26 at 18.

In opening new accounts, Respondent recorded demographic information on the BETA system. Tr. 577. Respondent checked the Specifically Designated Nationals and Blocked Persons List maintained by Treasury's Office of Foreign Asset Control ("OFAC"). If a customer's name was found on the list, the AML Manual required the AML compliance officer to follow whatever government directives were applicable. In addition, Respondent consulted the Financial Action Task Force's list of non-cooperative countries and territories to verify that the client was not doing business in any of them. CX-1 at 9 – 10; CX-26 at 11; Tr. 577 – 578.

Respondent used the Equifax service to verify basic customer information.[20] For example, Equifax checked a customer's social security number to see if the number had been issued to someone who was deceased, or if it was issued before the customer's date of birth. In addition, Respondent checked with the Compliance Data Center ("CDC"), an Equifax affiliate that monitors newspapers and other public information sources, and maintains a database of people with negative information. The CDC data included whether the subject of the report had been fined by FINRA. It also included any information maintained by state insurance regulators. Equifax also checked the OFAC list. CX-1 at 12; CX-22 at 3; Tr. 573 – 574, 577, 824. Sterne Agee forwarded CDC reports to the introducing firms. Tr. 582, 600. For foreign customers, Respondent required the introducing firms to obtain a copy of a government-issued picture identification document. Tr. 574 – 575.

3. Incoming Funds

The Central Cashiering Department (or Cash Management Department) was responsible for receiving all checks, and processing incoming and outgoing wires. Tr. 449, 458, 562. The 2003 AML Manual describes its primary AML responsibility as monitoring incoming wire transfer activity. CX-1 at 16. In 2004, Central Cashiering was required to monitor deposit activity other than incoming wire transfers, which were to be monitored by the Margin Department. CX-26 at 18.

4. Physical Certificates

The Legal Transfer Department examined the physical certificates received by Sterne Agee to determine if they were free to trade and to look for obvious fraud or forgery. Tr. 562.

[20] Equifax is widely used for AML monitoring. Tr. 824 – 825. Guidance from FINRA suggests Equifax as a source of information concerning customers' backgrounds for use at the time of account opening. NTM 02-21.

5. Outgoing Wires, Journals

The Margin Department was responsible for ensuring that all cash and margin accounts were kept in accordance with applicable rules and regulations. The Margin Department would review and approve all outgoing wires, cash journals, and securities journals. Tr. 458 – 459, 562.

Respondent's practice was that journal transfers required a letter of authorization from the client for journal transfers to a different customer's account. For accounts with the same ownership, customers could request journal transfers by e-mail. Tr. 470 – 471, 496 – 497. If a journal transfer was between different customers, it had to be approved by a supervisor or the risk division manager. Tr. 497.

When the Margin Department received a request to send money out of an account, it would do a "total account evaluation." The margin clerks looked at the history of the account to verify that everything in the account was acceptable. The review considered risk, any applicable rules or procedures, and AML requirements. The clerks reviewed the history of the account on the BETA system and the letters of authorization for the transaction. Sterne Agee's margin clerks maintained relationships with the particular introducing firms, and they discussed the accounts with their counterparts at the introducing firms. They were required to submit written requests for approvals of wire transfers to their supervisors. For domestic wires, a supervisor's signature was required, but above a certain level, a manager's signature was required. The risk division manager reviewed all requests for wire transfers, and also typically approved the requests. Tr. 459 – 463, 480 – 484, 488, 497, 521 – 522. The approval of the risk division manager or operations manager was required for all international wire transfers. CX-59 at 119 – 120.

6. Monitoring and Review by the AML Compliance Officer

Starting in 2004, the AML compliance officer created monthly activity reports for wire transfers. The reports tracked incoming and outgoing wires, and the number of wires sent during each month. CX-1 at 12; CX-22 at 10; Tr. 694. He also received a daily report of new accounts. Tr. 679. The AML compliance officer received daily reports with additional information, including incoming and outgoing wires, deposit and disbursement activity, and all transactions over $250,000. CX-59 at 31 – 34. Sterne Agee added more reviews as time went on. As an example, in about early 2005, Sterne Agee added a daily review of all trades over 25,000 shares. Tr. 695 – 696.

As noted above, the written procedures required Respondent's employees to report red flags, or any other suspicious or unusual account activity, to the AML compliance officer immediately upon detection. In practice, if the clerks saw something suspicious, they typically first reported it to their supervisors, and then to their department's manager. Tr. 499. Employees also would often bring matters directly to the attention of the AML compliance officer. When red flags were called to his attention, the AML compliance officer would conduct an investigation. CX-1 at 13, 15; CX-26 at 17; Tr. 461, 564, 567 – 570. For wires, he examined the trading to be sure that the trading supported the wire activity, and that money was not being passed through the account. He examined journal transfers to see why they were being done, and if the transfers made sense. Tr. 567.

D. Respondent's AML Training

Sterne Agee's AML program included a training component. Stip. 4. In 2003 – 2005, Sterne Agee's AML procedures stated that AML training would be satisfied through the Firm Element of Continuing Education. In 2003, the complete training program consisted of an online program offered by Bisys, a video, and a review of the firm's AML compliance manual. Stip. 5,

7; Tr. 211, 454 – 455, 556 – 557, 634 – 635, 683 – 684; RX-15; RX-18. In 2004 and 2005, the training used an online program provided by eMind rather than Bisys. Tr. 557 – 559; RX-1. There was no specialized training for the Operations Department as of July 11, 2005. CX-27 at 3.

The video discussed general AML principles, identified the general responsibilities of those departments with primary AML monitoring responsibilities, described the information that would be gathered for new accounts, and instructed employees to contact the AML compliance officer with AML issues. Tr. 214 – 221; CX-60. The training materials provided by Bisys and eMind discussed general AML principles. They were not specific to Respondent's business. RX-1; RX-15; RX-18.[21]

Sterne Agee kept its employees informed of their AML responsibilities through other measures in addition to the formal training program. Employees were required to certify that they had reviewed the firm's AML compliance manual, including updates. Tr. 557. The AML compliance officers had regular meetings with the managers. In turn, the managers trained the personnel who reported to them. Tr. 460 – 461, 480, 568, 644.

The Complaint alleges that the training for certain supervisors was inadequate because they received training only in conjunction with Respondent's annual compliance meeting, and therefore did not receive adequate training concerning the firm's money laundering risks, analysis of red flags, or the escalation of red flags. Timothy Vardaman, Sterne Agee's first AML compliance officer, became familiar with AML issues by attending Securities Industry Association ("SIA") and other seminars, talking to other firms, and talking to vendors. Tr. 451.

---

[21] While it might have been appropriate to provide training that was more tailored to Respondent's business and with a focus on the AML responsibilities of the various departments and employees, the Complaint does not allege that the overall training was deficient for failing to address the specifics of Respondent's business. At some time after 2005, Respondent started providing additional eMind training for Operations Department staff. Tr. 687.

Michael Keener became Sterne Agee's AML compliance officer in July 2003. Tr. 552. Keener had never been an AML compliance officer before he assumed the responsibility for Sterne Agee. He had been in the securities industry for nearly 20 years, but had no previous specialized AML training. Tr. 553 – 554, 632 – 633; CX-52 at 19. To learn how to perform his duties, Keener met with Vardaman, read materials on AML, went to a meeting on AML issues with the provider of the BETA software, participated in the BETA software provider's regulatory conference calls and NASD phone-in workshops, and participated in an SIA webcast on AML issues. Tr. 456, 555 – 556, 559, 702, 734 – 735; CX-52 at 19. Earl Bukolt, the Chief Operating Officer, attended several AML workshops given by the SIA but did not complete the Firm Element. Tr. 254 – 256; CX-43; RX-9.

In 2003, four margin clerks and a margin supervisor did not attend an AML training session, although all of Respondent's employees were required to attend. Stip. 6; Tr. 523; CX-57 at 81. Each of the five who missed the training later confirmed to the AML compliance officer that he or she had reviewed Respondent's AML policies. Tr. 704, 736.

E. Several Related Accounts Introduced by the Introducing Firm

The Complaint charges that the alleged weaknesses in Respondent's AML procedures and training resulted in its failure to file a Suspicious Activity Report with FinCEN within 30 days after the date of the detection of facts constituting a basis for filing a Suspicious Activity Report, as required by 31 C.F.R. § 103.19. In particular, the Complaint alleges that Respondent should have filed a SAR sooner with respect to several accounts introduced to Sterne Agee by a particular introducing firm (the "Introducing Firm").

1. Opening of the Introduced Accounts

In 2004, several accounts were introduced to Respondent by the Introducing Firm (the "Introduced Accounts"). Most of the Introduced Accounts were domiciled in an offshore

jurisdiction, and reflected the same foreign national as a person with trading authority. Stip. 10, 14. A U.S. national (the "U.S. National") had trading authority on several accounts. CX-5; CX-6; CX-18.[22] Some accounts maintained the same physical address. Stip. 12, 13.

Twice during 2004, Sterne Agee received advisory notices from Equifax reporting that the U.S. National had been the subject of a FINRA disciplinary action several years earlier. Stip. 16; CX-11; CX-19. Respondent's AML compliance officer received the Equifax reports, but did not consider the information that was in the reports to raise an AML risk. Tr. 599. The AML compliance officer forwarded the information to the Introducing Firm, and told the Introducing Firm that it was up to the Introducing Firm to accept or reject the account based on its knowledge of the account and the disclosure. CX-20; Tr. 599.

For the first of the Introduced Accounts, one of Respondent's employees reported to the new accounts manager that he had been unable to obtain customer identification information. CX-8; CX-9; Tr. 149 – 150. However, the AML compliance officer had no difficulty obtaining the customer identification information for this or other Introduced Accounts. Tr. 591 – 593, 651 – 654, 716.

2. Account Activity

The Introduced Accounts all exhibited similar activity. In each account, low-priced stocks were deposited, soon liquidated, and funds were wired out of the accounts. Tr. 78; CX-30 – CX-40. During 2004 through early 2005, securities were regularly deposited into one or another of the Introduced Accounts. Stip. 16. During that period, one or more of the Introduced Accounts were regularly among the top ten accounts on Sterne Agee's report of wire activity. Stip. 22; CX-22 at 30 – 36; Tr. 208 – 209. For the period 2004 through early 2005,

[22] The parties stipulated that the U.S. National had trading authority for some of the Introduced Accounts. Stip. 15. New account documentation shows that the U.S. National had trading authority on another account. CX-6; Tr. 70 – 71.

more than $100,000 was wired into the Introduced Accounts, and less than $50,000 was wired out of those accounts. Stip. 19. For the accounts domiciled in the offshore jurisdiction, the outgoing wires were directed to an account maintained at a United States financial institution, with further instructions that the funds be directed to an account maintained at an offshore financial institution, for credit to an account related to the foreign national. Stip. 20. The outgoing wires for one account were directed to an account maintained in the name of the owner of the account at a United States financial institution. Stip. 21.

The bulk of the securities deposited into the Introduced Accounts came in electronically. Tr. 488 – 489, 604. The stocks were not restricted at the time they were deposited in the Introduced Accounts. Tr. 680 – 681; CX-52 at 11. Respondent was reassured by the fact that it was not getting exception reports or returned securities when the stocks were sold, which indicated that the stocks met the good delivery standards of the next broker-dealer. CX-57 at 166 – 168.

During a brief period in 2004, one of the Introduced Accounts received several million shares of the XYZ Corporation [fictitious name] and continued to trade in the stock through early 2005. Stip. 17. There were no purchases of XYZ stock through Respondent. Tr. 80; CX-32. When the first of the XYZ shares were deposited, Respondent did due diligence to determine if the shares could be sold, pursuant to Respondent's regular practice with respect to deposits of more than 25,000 shares of any stock. Tr. 813 – 814. At the time the shares were deposited and sold, XYZ was a defendant in an SEC action. CX-4. Respondent was not aware of the SEC action at the time the XYZ shares were deposited, but became aware of it later. Tr. 667 – 668. Respondent ultimately determined that the stock was restricted and could not lawfully be sold. Tr. 815 – 816.

Shares of ABC, Inc. [fictitious name] were also deposited into the Introduced Accounts. Stip. 18. The SEC suspended trading in ABC for a brief period. CX-24; Tr. 239 – 240. The Introduced Accounts did not trade the stock while trading was suspended. Tr. 260, 606.

3. Monitoring the Introduced Accounts for Suspicious Activity

Respondent was well aware of the Introduced Accounts but for several months did not regard them as presenting a money laundering risk. Respondent regularly examined the accounts and found that there were reasonable business explanations for the activity in the accounts, consistent with the representations from the Introducing Firm and the U.S. National concerning the anticipated activity in the accounts.

Respondent was aware of the U.S. National and the nature of the business he would be doing with the Introducing Firm before the Introduced Accounts were opened. A Sterne Agee representative met with the Introducing Firm before the accounts were opened and was introduced to the U.S. National. The U.S. National and the Introducing Firm said the U.S. National was doing PIPE transactions.[23] Tr. 120 – 121, 124, 129 – 130, 186.

When the first of the Introduced Accounts was opened at Sterne Agee, Respondent's Legal Transfer Department checked the filings on the SEC's Edgar database with respect to the stocks that were deposited into the account. Legal Transfer also ran an SIC inquiry[24] on each certificate, and contacted the agent for each stock to verify that there were no stops or restrictions on the certificates. Legal Transfer concluded that the shares could be sold. Respondent required additional, original documents from the Introducing Firm before it notified the Introducing Firm

[23] "'PIPE' stands for 'private investment in public equity.' In a PIPE offering, investors commit to purchase a certain number of restricted shares from a company at a specified price. The company agrees, in turn, to file a resale registration statement so that the investors can resell the shares to the public." www.sec.gov/answers/pipeofferings.htm.

[24] The Securities Information Center runs the SEC's Lost and Stolen Securities Program where all lost, stolen, missing, and counterfeit certificates are reported. *See* www.secic.com.

that the stock could be sold. RX-6. Soon after the first of the accounts was opened, Respondent received private placement memoranda for the first couple of PIPE transactions. Respondent concluded that the shares had been legitimately acquired by the clients. CX-56 at 89 – 92. Shortly after the accounts were opened, Operations notified the AML compliance officer about wire activity in the accounts. Tr. 594.

The risk division manager spoke to the Introducing Firm regularly about the Introduced Accounts. The AML compliance officer and others were involved in frequent discussions about the accounts. Tr. 485 – 487, 489 – 495, 504, 508, 595, 597. The accounts were discussed at the Ad Hoc Credit Committee in 2004, and Respondent monitored the accounts closely. Tr. 674 – 675, 724 – 725.

The AML compliance officer reviewed the Introduced Accounts regularly, and concluded that the activity in the accounts was what Respondent had been told it would be, that the activity in the accounts made sense, and that it was consistent with the Introducing Firm's representation that the accounts would engage in PIPE transactions. Tr. 594, 596, 660. The Introducing Firm had told Respondent that the client would purchase securities at a discount, deposit a large number of securities that would be sold once it was permissible, and the proceeds would be wired out. Tr. 594, 680 – 681, 737 – 738. The Introducing Firm had explained that the different accounts were related to different securities and different groups of investors. Tr. 597 – 598, 745. Although there were many wires to the offshore jurisdiction, the wire activity was consistent with the Introducing Firm's representation that the accounts would be depositing securities, selling them, and wiring funds out. The funds were all wired to the same bank, with the same signatory on the account. The funds all went to the bank for credit to the entity that initiated the wire. If the wire was initiated by the sale of securities for the owner of one of the

accounts, the wire went to the owner of that account. There were no incoming wires and minimal journal transfers. Tr. 602 – 604. Respondent concluded that there was no "layering of funds." Tr. 603.[25]

As discussed below, Respondent filed a SAR with respect to the Introduced Accounts on February 10, 2005. On June 9, 2005, Keener sent an e-mail to the Introducing Firm, noting that five of the accounts had large transaction and wire volumes, and asking the Introducing Firm to take a look at the accounts and send Respondent a written explanation of the accounts' activities. CX-25 at 1. In response, the Introducing Firm forwarded an e-mail from the U.S. National to the Introducing Firm, saying that there was documentation concerning the transactions, and all transactions were compliant with requirements of the securities laws. CX-25 at 3.

4. Respondent Filed Two Suspicious Activity Reports Concerning the Introduced Accounts

On October 12, 2004, AmSouth Bank, which was located in Birmingham, Alabama, entered into a settlement with FinCEN, consenting to the imposition of a civil penalty of $10 million for its alleged failure to develop an adequate anti-money laundering program, resulting in the failure to file timely SARs.[26] The *AmSouth* settlement led to discussions at Sterne Agee concerning the AML requirements, and a broadening of Sterne Agee's view of what was reportable. These discussions led to the decision to file a SAR with respect to the Introduced Accounts. Tr. 607 – 609; CX-21.

[25] Money laundering is often described as occurring in three stages. At the "placement" stage, the cash first enters the financial system and is converted into monetary instruments or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy. NTM 02-21, at 1.

[26] FinCEN press release, in the hearing record at CX-21; *see also AmSouth Bank*, FinCEN, Dkt. No. 2004-2, available on FinCEN website.

Respondent filed a SAR with respect to the Introduced Accounts in early 2005. Stip. 24. The SAR was filed because of the level of wire activity, the fact that they were foreign accounts, and because of the repetitive nature of the transactions, which had gone on for months. Tr. 607 – 609; CX-57 at 152. The account activity remained essentially unchanged after Respondent filed the first SAR. Tr. 249. A second SAR was filed later in 2005. Stip. 24.

F. Conclusions of Law for Violation Charged for 2002 through 2005

Enforcement bears the burden of proving by a preponderance of the evidence that Respondent violated Conduct Rule 3011 by failing to "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under 31 U.S.C. § 5318(g) and the implementing regulations thereunder."[27] The Hearing Panel finds that Enforcement failed to meet its burden of proof.

1. Respondent's System of Monitoring Transactions in 2002 through 2005 Was Reasonable

The central issue with respect to Respondent's AML program for 2002 through 2005 was Respondent's use of a largely manual system. There is little guidance on the degree of automation that would be required under the Patriot Act and Conduct Rule 3011 as part of a reasonable AML program for a securities firm for 2002 through 2005. In its April 2002 Notice to Members, FINRA stated that clearing firms should have automated systems. NTM 02-21, at 15. The NTM had no further discussion of the type or degree of automation that clearing firms should have.

Both parties offered expert testimony in support of their positions on the adequacy of Respondent's AML program. Both experts were highly qualified to testify concerning AML

[27] *See Dep't of Enforcement v. Respondent*, No. C9B040020, 2006 NASD Discip. LEXIS 28, at *11 – *12 (N.A.C. Aug. 8, 2006) (affirming Hearing Panel's dismissal of case against supervisor for failure to exercise reasonable supervision under NASD Conduct Rule 3010).

procedures for the securities industry, but the Hearing Panel finds the opinions of Respondent's expert concerning Respondent's AML compliance for April 2002 through July 2005 more reasonable.

Enforcement's expert witness, Judith Poppalardo, took the position that Respondent's AML procedures were inadequate because Respondent relied on a manual system. In her opinion, the nature of Respondent's business made a manual system inadequate. She testified that a manual system would be inadequate for all but very small firms, and that only a more automated system could identify patterns and links among accounts. Tr. 360 – 361, 381 – 382, 398, 427, 429, 865. She testified that there were a number of AML software programs available. Tr. 365 – 367. She estimated the costs for Respondent to have implemented the type of automated system she regarded as necessary at $500,000 to purchase the software, $150,000 to $200,000 for start-up expenses, plus annual software licensing fees. She testified that the software would have required customization, and that Respondent would have had to work with vendors for "upwards of a year" to implement an automated system. Tr. 367 – 369, 430.

Respondent's expert, Peter Djinis, disagreed. He testified that many firms still rely on the types of AML procedures employed by Respondent, and that Respondent's reliance on such methods was reasonable. Tr. 771 – 772, 774. Furthermore, he testified that there were not many AML software programs available for the securities industry in 2002 and 2003. Tr. 766, 770 – 771. The programs that were available at the time were geared toward the largest firms, and the implementation of AML software at the time was a "multi-million dollar investment." Tr. 766 – 767.

The Hearing Panel finds that, for the period covered by the allegations in the Complaint, Respondent's AML policies and procedures could be reasonably expected to detect and cause the

reporting of suspicious activity and transactions, as required by Conduct Rule 3011(a).[28] The Hearing Panel reaches this conclusion for a number of reasons. First, the foundation for Enforcement's case is the contention that Respondent's AML policies and procedures were deficient because Respondent's AML program was not automated to the degree advocated by Enforcement. While it is likely that a well-functioning automated system would have identified certain patterns that would not have been identified during a manual review, Enforcement has not shown that it was unreasonable not to have a more automated system in 2003 through 2005. Enforcement did not establish that there was proven, reliable software available for Respondent's clearing business during the relevant time period. Respondent purchased AML software and used it for several months before discovering that the software did not monitor its clearing business. The requirement for securities firms to have AML procedures was new, and, as Respondent's experience demonstrates, AML software was far from certain to work for Respondent's business. Enforcement also did not establish that Respondent's mix of manual and automated monitoring missed suspicious transactions that an automated system would have caught.

Second, the AML software that was on the market at that time was expensive and burdensome to implement. The focus of an AML compliance program should be "a risk-based

---

[28] The Hearing Panel's finding is applicable from April 24, 2002, through July 11, 2005, the period covered by the allegations in the Complaint. AML procedures, enforcement, and technology have been something of a trial and error process, and have evolved, and will continue to evolve. *See, e.g.*, "Money Laundering: Life After the PATRIOT Act," Speech by Lori Richards, Director, Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, at the SIA Conference on Anti-Money Laundering Compliance for Broker-Dealers (May 2, 2002) (available on SEC website at www.sec.gov/news/speech/spch555.htm). Respondent's expert testified that there has been an evolutionary process in procedures, products offered, and enforcement since AML procedures first became required for the securities industry. Tr. 771. FINRA similarly noted in 2002, "Anti-money laundering is an evolving topic that places additional due diligence and reporting responsibilities on firms, supervisors, and registered representatives." NTM 02-70 (Oct. 2002). In fact, as noted in this decision, Respondent's processes have evolved significantly, and continue to evolve. *See, e.g.*, Tr. 696 – 697. Respondent has implemented the use of a variety of reports using BETA Access in recent years. Tr. 708 – 712. The Hearing Panel makes no finding with respect to the level of automation that might be required in 2010.

approach to developing compliance procedures that can be reasonably expected to promote the detection and reporting of suspicious activity."[29] Thus, it is appropriate to consider the cost of implementation in determining whether particular AML detection measures are required. Enforcement has failed to show that Respondent's AML monitoring and reporting procedures were not appropriate for the level of risk faced by Respondent in its clearing business.

Third, and most importantly, Respondent's AML compliance efforts were substantial, and its AML program could reasonably be expected to, and did, detect suspicious activity. The Operations Department staff was required to identify the types of red flags that related to their respective duties. The Operations Department personnel were assigned tasks that were sufficiently well defined and within their specific areas of responsibility that they could be expected to spot suspicious activity. The record shows that they brought potential red flags to the attention of their supervisors and, where appropriate, the AML compliance officer. Respondent detected the only transactions that Enforcement has identified as suspicious transactions, and filed two SARs with respect to those transactions.

Respondent employed a full-time AML compliance officer who reviewed matters brought to his attention, and conducted reviews to detect possible money-laundering activity. Respondent was able to compile a substantial amount of information using BETA and BETA Access, including some information that AML software programs could not generate. It gathered the types of information that were reasonably available to a clearing firm. The Equifax reports provided information concerning the identity and background of its customers, including

[29] NTM 02-21, citing Financial Crimes Enforcement Network, *Proposed Amendment to the Bank Secrecy Act Regulations – Requirement of Brokers or Dealers in Securities to Report Suspicious Transactions*, 66 Fed. Reg. 67670 at 67674 (Dec. 31, 2001); *see also Bank Secrecy Act Effectiveness and Efficiency Fact Sheet*, available at www.fincen.gov/news_room/rp/rulings/pdf/bsa_fact_sheet.pdf (Jan. 2007) (stating that FinCEN would initiate an effort "to ensure that financial institutions and regulators treat compliance obligations in a manner that helps to avoid expenditures that are not commensurate with actual risk").

whether the customers or countries were on OFAC or Financial Action Task Force lists. The AML compliance officer received or created reports concerning new accounts, deposits and disbursement activity, all transactions over $250,000, stock transactions of more than 25,000 shares, and wire transfers. The firm filed 19 SARs from September 20, 2003, through July 8, 2005. Tr. 846 – 847.

The Hearing Panel finds that Enforcement has not carried its burden of proving that Respondent's procedures were inadequate to detect potential red flags. Between the initial efforts of the Operations Department staff and the reports reviewed by the AML compliance officer, the program was reasonably designed to detect potential money laundering transactions.

2. Respondent's Written Procedures Adequately Described How to Identify and Review Transactions, and How to Escalate Red Flags

The Complaint alleges that Respondent's written AML procedures "should have provided instructions to … employees about how to identify and review transactions for anti-money laundering red flags and should have set forth a description of the method for escalating these red flags for additional investigation and reporting if appropriate." The Complaint alleges that the procedures "did little more than identify the operational departments responsible for review and the general areas that should be reviewed."

The Hearing Panel finds that Respondent's procedures adequately described how to identify and review transactions, and how to escalate red flags. The procedures identified the various departments within the Risk Division that would review transactions, and the issues for which each department would conduct a review. The descriptions were reasonably specific, and, in conjunction with the list of red flags, provided the clerical staff with sufficient direction to enable them to spot red flags. The kind of additional detail that Enforcement advocates is operational detail that was unnecessary for the written AML procedures.

The escalation procedures were also set forth clearly in the written procedures. The AML Manual repeatedly advised Respondent's staff to bring AML issues to the attention of the AML compliance officer.

Enforcement has not identified any procedures that were missing from the written procedures, nor has it shown that the Operations Department staff had any difficulty in understanding what would constitute a red flag that should be brought to the attention of their supervisors or the AML compliance officer. The Hearing Panel finds that Enforcement failed to show by a preponderance of the evidence that Respondent's written procedures were inadequate to provide the guidance necessary to advise Sterne Agee's staff of their AML duties.

3. Respondent's Training Program Was Reasonable

Conduct Rule 3011(e) requires FINRA members to provide "ongoing training for appropriate personnel." The Complaint alleges that Respondent's AML training was inadequate. In particular, the Complaint, as explained in Enforcement's pre-hearing brief, alleges that the overall training program failed to address the method for identifying red flags and failed to address the role of the employees with specific AML responsibilities.[30] The Complaint alleges that the training for certain members of management with AML responsibilities – the "Risk Division Manager & Anti-Money Laundering Compliance Officer," and the chief operating officer – was inadequate because they received only the training available to all employees, but should have received additional training that was more specific to Respondent's business. The Complaint also alleges that these three employees[31] received no training on how to escalate transactions for further investigation and the filing of suspicious activity reports. The Complaint

[30] Complaint, ¶19; Department of Enforcement's Pre-Hearing Brief, at 24.

[31] It is unclear whether the Complaint refers to two employees or three employees, but both parties presented evidence concerning three employees.

charges that Respondent's AML training program for the rest of its employees was "similarly inadequate."

The core of Respondent's formal training program were the video and the online program provided by Bisys in 2003, followed in 2004 by the similar program provided by eMind. Enforcement's expert testified that the Bisys materials were very good, but that the video "could have been better" because she "would have liked" more specific direction on transaction monitoring by each department. Tr. 393 – 395.

Enforcement's contention that there should have been more specialized training for certain employees is unsupported. The video provided a useful introduction to Respondent's AML procedures. The Bisys and eMind materials supplemented the video, and provided additional, more detailed information on the overall AML issues for securities firms.[32] The overall training was more than sufficient to educate the Operations Department staff on their specific responsibilities. The responsibilities were allocated to the various departments within Operations, such as Legal Transfer and the Margin Department. The AML responsibilities were consistent with their regular duties, and were sufficiently narrow that the employees did not require further training to spot the red flags appropriate to their departments, especially in light of the frequent departmental meetings at which AML issues were discussed.[33]

In addition, Enforcement did not show any deficiencies in the training of the three management persons. Earl Bukolt, the chief operating officer, attended a number of AML workshops for securities firms. There is no direct evidence concerning his AML duties, or what

---

[32] Respondent's employees also received additional, less formal guidance on their AML responsibilities. Employees were required to certify that they had read Respondent's AML Manual. Employees at all levels of the Operations Department met regularly, and those meetings included discussions of AML issues.

[33] As Mr. Djinis noted, there were few people with AML experience in the brokerage industry in 2003. There is no evidence that more specialized training was available. Tr. 825.

training was missing with respect to those duties. Enforcement did not show that he was insufficiently trained to perform whatever supervisory AML duties he may have had.

Timothy Vardaman was well trained to assume his duties as the first AML compliance officer. He attended a number of workshops and seminars, and spoke to other firms and to vendors. Enforcement did not show that Vardaman was inadequately trained to perform his AML duties. Additionally, there is no evidence that there was additional training available in 2002 for the securities industry that would have enhanced Vardaman's ability to perform his AML duties.

Michael Keener was also well trained. He worked with Vardaman, attended AML programs, read AML materials, and participated in telephone programs on AML. The Hearing Panel finds that the training for Vardaman and Keener was sufficient and appropriate for their AML duties as of 2002 and 2003. Enforcement has not shown that Bukolt was inadequately trained because it has presented little evidence of the training he received, and virtually no evidence of his AML responsibilities. Enforcement failed to sustain its burden of proof.

4. The Failure of Five Employees to Participate in the Training Program in 2003

In 2003, five members of the Margin Department did not complete AML training. As Mr. Vardaman testified, the Margin Department was "one of the front lines of defense" for Respondent's AML program. Tr. 460. Respondent should have taken steps to ensure that all of its employees with any AML responsibility attended training, and should have been especially careful to ensure the attendance of those with such important AML responsibilities. Although this was a failure by Respondent to enforce its own AML requirements as well as to train certain key employees, this failure by itself is insufficient to support a finding that the AML program as a whole was inadequate in 2002 – 2005, as charged in the Complaint. There is no evidence that

these employees did not understand their AML responsibilities, that they missed training again, or that any other employees ever missed the training.[34]

5. The Monitoring of the Introduced Accounts and Timing of the SAR Filings Do Not Establish that the AML Program Was Deficient

Enforcement contends that the alleged weaknesses in Respondent's AML procedures resulted in late filing of suspicious activity reports for the Introduced Accounts. The first SAR was filed for the Introduced Accounts in early 2005, but Enforcement's expert testified that the SAR should have been filed by about July 2004. Tr. 380, 416 – 417. She testified that there were numerous AML red flags, and that if Respondent had conducted a more thorough examination, such as using the SEC's Edgar service to look for registration statements for the securities traded by the accounts, it would have found that there was no genuine business purpose for the transactions in the Introduced Accounts. Tr. 372, 387, 389, 392 – 393, 404, 421, 853, 879.

Respondent's expert disagreed. He emphasized that, in his opinion, Respondent's process of monitoring the Introduced Accounts was sound. Respondent monitored the accounts, performed due diligence, and ultimately filed two SARs. Tr. 791 – 793, 797 – 798. In his view, Respondent did not have to file a SAR for the Introduced Accounts, but it was prudent to do so. Tr. 832 – 834. He testified that the decision to file a SAR is subjective and not based on a mathematical formula. He testified that what is important is that Respondent had a process to detect suspicious activity. Tr. 830 – 831.

The testimony of Respondent's expert was more persuasive and more consistent with the applicable legal standards. The Federal Financial Institutions Examination Council ("FFIEC")

---

[34] All five employees certified that they had read the AML Manual in 2003, and that they regularly attended meetings with their supervisors in which AML issues were discussed.

has emphasized the importance of focusing on the process, rather than on whether a particular SAR was filed. In its examination manual for banks, FFIEC states, "The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions."[35] This is not to say that the failure to file a SAR cannot be questioned, and FINRA has settled matters involving the failure to file SARs.[36]

Respondent's procedures in monitoring the Introduced Accounts were sound and support the Hearing Panel's finding that the overall AML program was sound. Respondent was aware of the Introduced Accounts, regularly monitored them, and regularly communicated with the Introducing Firm about the accounts. While finding some red flags, it made a reasonable determination that it was not appropriate to file a SAR until the cumulative activity, plus a changed view of the regulatory climate, caused sufficient concerns to prompt the filing of a SAR.

Respondent was aware of almost every issue raised by Enforcement with respect to the Introduced Accounts. It was aware of the U.S. National's disciplinary history, but it did not regard it as a money-laundering risk because it involved a matter that had been resolved several years earlier, and because of the nature of the matter.

Respondent knew that several of the accounts were domiciled in an offshore jurisdiction; that large blocks of stock were being deposited and liquidated; and that the proceeds of the sales

---

[35] Federal Financial Institutions Examination Council, "Suspicious Activity Reporting – Overview," *Bank Secrecy Act Anti-Money Laundering Examination Manual*, available online at www.ffiec.gov, and linked through www.finra.org/Industry/Issues/AML; *see also* "Amendment to the Bank Secrecy Act Regulations – Exemptions from the Requirement to Report Transactions in Currency," 73 Fed. Reg., No. 235, page 74010, 74011 (Dec. 5, 2008) (noting that a SAR requires a financial institution to make a subjective determination of what is suspicious); Statement of William F. Baity, Deputy Director, FinCEN, May 10, 2007, before the House Financial Services Subcommittee on Oversight and Investigations, available at http://www.fincen.gov/news_room/testimony/html/20070510.html ("Financial institutions file Suspicious Activity Reports (SARs) after a subjective review of numerous variables ….")

[36] *See, e.g.*, *Cambria Capital, LLC*, No. 2007007402901 (reported in Feb. 2009 Disciplinary and Other FINRA Actions) (available on FINRA website); *James Russell McCarthy, Jr.*, No. 2006003916902) (reported in May 2009 Disciplinary and Other FINRA Actions) (available on FINRA website).

were being wired to offshore accounts. The AML compliance officer looked into the activity, and concluded that there was a reasonable business explanation for all of it, consistent with the representations from the Introducing Firm and the U.S. National that the accounts were going to be used for PIPE transactions.

Enforcement contends that Respondent should have gone farther in investigating the accounts. For example, Respondent was not aware that XYZ was a defendant in a case brought by the SEC. While Respondent might have learned more with further investigation, its investigation was adequate under the facts and circumstances of this case. Sterne Agee obtained a substantial amount of information about these accounts, monitored them, discussed them, and came to a reasonable conclusion that there was a reasonable business explanation for the activity in the accounts. Enforcement has provided no authority for any requirement to go beyond the sources of information that Sterne Agee used, and conduct Internet searches under these circumstances.

Respondent's regular monitoring and evaluation of the Introduced Accounts, and the filing of SARs, support the reasonableness of Respondent's AML procedures.

6. Conclusion: The Overall AML Program for 2002 through 2005 Was Reasonable

The Hearing Panel finds that for the period April 24, 2002, through July 11, 2005, Respondent established and implemented policies and procedures that were reasonably expected to detect and cause the reporting of transactions required under the BSA and the implementing regulations thereunder.

IV. Violation Charged with Respect to AML Program in 2006 and 2007

The Complaint alleges that because of certain specific deficiencies in its AML program, Respondent failed to develop and implement a written AML program reasonably designed to

achieve and monitor the firm's compliance with the BSA from July 1, 2006, through April 20, 2007. According to the Complaint, Respondent had no procedures to monitor for suspicious activity related to physical securities certificates or journal transfers of shares or funds; failed to establish and implement procedures to identify direct accounts for foreign financial institutions and to identify and mitigate the risk of such accounts; and failed to obtain foreign bank certifications for nine (later changed to five) accounts, as required by the Patriot Act. As a result of the alleged failure to detect foreign bank accounts, Respondent allegedly failed to provide notices required by federal regulations regarding transactions with the Bank of Syria, VEF Banka, and Banco Delta Asia. Finally, the Complaint alleges that during this period, Respondent failed to establish and maintain an adequate customer identification program for delivery versus payment ("DVP") accounts.

The Hearing Panel finds that Respondent violated Conduct Rules 3011 and 2110, and MSRB Rule G-41, because the AML program for this period had certain of the deficiencies charged in the Complaint, as set forth below.

A. Respondent's Procedures for Reviewing Physical Securities Certificates Were Reasonable

The Complaint alleges that Respondent did not have written procedures or a system in place to monitor for suspicious activity related to physical securities certificates, a "risk area[] for detecting possible money laundering or other suspicious activity."

Respondent did not have specific written procedures in place to monitor for suspicious activity related to physical securities certificates from July 1, 2006, through April 20, 2007. CX-44; CX-45; CX-54. However, in practice, Respondent reviewed all securities deposited in client accounts. Tr. 470. Throughout the periods covered by the Complaint, Respondent's policy was that if any account received more than 25,000 shares in a 30-day period, the customer was

required to provide letters from the individual account owner, the transfer agent, and from the issuer, stating that the securities were free to trade. Tr. 144 – 146, 287, 604 – 605. Furthermore, as noted above, the Legal Transfer Department examined the physical certificates coming in, to determine if they were free to trade, and to look for obvious fraud or forgery. Tr. 562.

The Hearing Panel finds that Respondent's written AML procedures with respect to the deposit of physical securities certificates in 2006 and 2007 were adequate, and that, for the time period charged in the Complaint, a specific requirement in the written AML procedures to review physical securities is the kind of operational detail that was not required. Enforcement has not shown that a written AML procedure for the review of physical securities certificates was required to be part of Respondent's AML procedures.[37]

The Hearing Panel also finds that Respondent's practices for review of physical securities certificates were reasonable. The procedures would likely have identified the attempted sale of securities that could not be freely traded, the most significant money-laundering risk with respect to the deposit of physical securities. Enforcement has not identified any specific money-laundering activities that were unlikely to be detected by Respondent's procedures.

B. Respondent's Procedures for Monitoring Journal Transfers Were Reasonable

The Complaint alleges that Respondent did not have written procedures or a system in place to monitor for journal transfers of shares or funds, a "risk area[] for detecting possible money laundering or other suspicious activity."

[37] In a recent regulatory notice, FINRA stated that the opening of a new account into which a customer delivers physical certificates representing a large block of thinly traded or low-priced stocks has recently been identified as a red flag that might signal the possibility of an illegal, unregistered stock distribution. Reg. Notice 09-05 (Jan. 2009). Enforcement has not identified any regulatory notices that identified the deposit of physical securities as an AML red flag that should have been in a firm's AML procedures in 2007. It was not identified as a red flag in NTM 02-21.

The AML Manuals for 2006 and 2007 provided that if any member of the staff of the Margin Department "notices any activity including but not limited to … money journals, security journals … that appear to be out of the ordinary" he or she should notify the AML compliance officer. CX-44 at 14; CX-45 at 15. In addition, excessive journal transfers between unrelated accounts without any apparent business purpose were identified as a red flag in Respondent's AML Manuals. CX-44 at 16; CX-45 at 18. In 2006 – 2007, Sterne Agee's general written policy prohibited journal transfers. The policy was not an AML-specific policy, and was not part of the written AML procedures. Tr. 622; CX-44; CX-45.

The Hearing Panel finds that the written procedures for journal transfers were adequate, and provided sufficient guidance to the Operational Department staff in the detection of possible money-laundering activity, especially given Respondent's general prohibition against such transfers.[38] Enforcement has not identified any procedures that were lacking from the written AML procedures that would have been necessary to provide Respondent's personnel with all the information they needed to perform their AML duties.

C. Respondent's Procedures for Identifying Direct Foreign Financial Institution Accounts Were Reasonable

The Complaint alleges that Respondent did not have adequate procedures for identifying its direct accounts for foreign financial institutions.

Respondent did not have many direct foreign financial institution accounts. Tr. 614. Its AML Manuals for 2006 and 2007 required Sterne Agee to detect correspondent accounts for foreign shell banks, to obtain certifications for foreign bank account holders, and to keep records identifying the owners of foreign banks with the U.S. correspondent accounts. CX-44 at 11; CX-

[38] There is no evidence that there were any journal transfers between July 1, 2006, through April 20, 2007. In light of the general prohibition, the procedures were adequate to detect money-laundering issues if any exceptions to the general prohibition were permitted.

45 at 12 – 13. To implement these procedures, it would have been necessary to identify all accounts for foreign financial institutions. In 2006 and 2007, Respondent used BETA Access to create lists from which it identified foreign financial institutions. Respondent first identified all accounts that did not have zip codes. Affiliate accounts were examined to identify names that sounded like foreign banks. Tr. 613 – 614, 697; CX-51.[39]

The Hearing Panel finds that Respondent's written procedures in 2006 and 2007 were reasonable, and that Enforcement failed to show that the procedures were inadequate to inform Respondent's staff of their AML duties. The Hearing Panel also finds that the procedures followed were reasonable. Although, as discussed below, some foreign financial institution accounts were missed, the procedures were reasonably designed to detect such accounts.

D. Respondent's AML Procedures Were Deficient in Their Implementation Because Respondent Failed to Detect and Obtain Certifications or Equivalent Information for Certain Foreign Banks, and Failed to Send the Notifications Required by Section 311 of the Patriot Act to Those Banks

The Complaint alleges that Respondent failed to detect certain foreign banks, and therefore did not obtain foreign bank certifications. As a result, Respondent failed to provide notices required by Section 311 of the Patriot Act.

The parties stipulated that Respondent did not obtain foreign bank certifications or otherwise obtain the equivalent information for three accounts for foreign banks: two for UBank, and one for Next Century Investors. Stip. 25. The implementation of Respondent's AML procedures was deficient because Respondent failed to obtain bank certifications or the

[39] The Complaint charges a failure to identify foreign financial institutions only for direct accounts maintained at Respondent's affiliates, and not for introduced accounts cleared by Sterne Agee.

equivalent information for UBank or Next Century, as required by the regulations implementing Sections 313 and 319 of the Patriot Act.[40]

Respondent also did not maintain a copy of the bank certification for the Bank of Montreal, a foreign bank that maintained five accounts at Sterne Agee. Tr. 301 – 305, 307, 618 – 619, 698; CX-47. Enforcement did not establish that Respondent failed to obtain the equivalent information for the Bank of Montreal. However, Respondent's AML procedures required it to obtain foreign bank certifications for all accounts maintained by foreign banks. CX-44 at 11; CX-45 at 12. Accordingly, Respondent's failure to obtain the certification for the Bank of Montreal violated NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41.

Section 311 of the Patriot Act added section 5318A to the BSA, granting the Secretary of the Treasury the authority to require domestic financial institutions and domestic financial agencies to take certain "special measures" after finding that reasonable grounds exist for concluding that a foreign jurisdiction, foreign financial institution, international class of transactions, or type of account is of "primary money laundering concern." *See, e.g.*, NTM 06-41 (Aug. 2006). Special measures have been instituted with respect to the Bank of Syria, VEF Banka, and Banco Delta Asia.[41] Because Respondent did not identify the accounts for UBank,

---

[40] 31 C.F.R. §103.177. Section 313 of the Patriot Act prohibits broker-dealers from establishing, maintaining, administering, or managing a correspondent account on behalf of a foreign shell bank. Section 319 requires broker-dealers to maintain records identifying the owners of foreign banks for which correspondent accounts are maintained and the name and address of a U.S. resident authorized to accept service of legal process for records regarding such correspondent accounts, and take reasonable steps to ensure that the accounts are not being used indirectly to provide services to a foreign shell bank. *See* FinCEN, FIN-2006-G003 (Feb. 3, 2006). NTM 02-21 recommended that broker-dealers require their foreign bank account holders to complete certifications. Effective October 28, 2002, FinCEN adopted regulations implementing both provisions. The regulations allow broker-dealers, and other covered financial institutions, to receive a safe harbor for compliance with Sections 313 and 319 if they use the certification process described in the regulation. *See* Anti-Money Laundering Requirements – Correspondent Accounts for Foreign Shell Banks; Recordkeeping and Termination of Correspondent Accounts for Foreign Banks, 67 Fed. Reg. 60562 (Sept. 26, 2002). Respondent failed to obtain the information required by the statute, or obtain the certifications to take advantage of the safe harbor.

[41] 31 C.F.R. §103.188; 31 C.F.R. §103.192; 31 C.F.R. §103.193.

Next Century, or the Bank of Montreal, Respondent failed to send the special measures notices required by the regulations, thereby violating NASD Conduct Rule 3011. CX-46; Tr. 621 – 622.

E. Respondent's AML Procedures Were Deficient Because Respondent Did Not Have Written Procedures to Comply with Section 312 of the Patriot Act

The Complaint alleges that Respondent did not have adequate procedures for "conducting the required due diligence to analyze the risk and implementing procedures to mitigate the risk as required by Section 312 and the implementing regulations."

Section 312 of the Patriot Act requires each U.S. financial institution, including securities brokers, to "establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering" through correspondent accounts maintained for foreign financial institutions.[42] FinCEN's rule implementing Section 312 of the Patriot Act provides that securities firms must "[assess] the money laundering risk presented by such correspondent account, based on a consideration of all relevant factors, which shall include, as appropriate," five factors specified in the rule.[43]

Although the regulations under Section 312 were not issued until 2006, FINRA alerted its members to the statutory requirement as early as April 2002. NTM 02-21. The NTM stated, "Regardless of whether final regulations have been promulgated, the minimum due diligence requirements set forth in Section 312 … become ***effective on July 23, 2002.***" (emphasis in original).

---

[42] Anti-Money Laundering Programs; Special Due Diligence Programs for Certain Foreign Financial Accounts; Final Rule and Proposed Rule, 71 Fed. Reg. 496 (Jan. 4, 2006); 31 C.F.R. §103.176(a)(2).

[43] 31 C.F.R. §103.176(a)(2). The rule requires application of only those factors that are relevant to each account. FinCEN, "Application of Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industry," FIN-2006-G009, May 10, 2006.

Respondent's AML Manuals for 2006 and 2007 do not mention the requirements of Section 312, and contain no procedures that would implement the requirements of FinCEN's rules implementing Section 312. CX-44; CX-45. In its March 30, 2007, response to the comments at the exit interview for a FINRA examination, Respondent acknowledged that its written procedures do not address the rules under Section 312. CX-54 at 1.

Respondent's written AML procedures violated NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41, because they failed to include procedures to comply with Section 312 of the Patriot Act.

F. Respondents AML Procedures in 2006 and 2007 Were Unreasonable Because Respondent Failed to Implement Customer Identification Procedures for Delivery Versus Payment Accounts

The Complaint alleges that during the period July 1, 2006, through April 20, 2007, Respondent failed to establish and maintain an adequate customer identification program for delivery versus payment accounts.

In a DVP transaction, the delivery of securities occurs simultaneously with payment. The delivery and payment take place at a custodian institution, such as the Depository Trust Company. In a DVP transaction, the clearing firm essentially acts as a matchmaker, matching up those who have custody over the securities and those who have custody over the funds to make sure that simultaneous sales can occur and the proceeds can be received as contracted. Tr. 609 – 610, 802.

Respondent's AML Manual recognized the need for customer identification procedures for DVP accounts, stating that it would require less customer identification documentation for accounts that settle trades DVP because Respondent does not maintain cash or securities, and accounts are usually kept by larger institutional customers who are subject to the Patriot Act. CX-44 at 7; CX-45 at 7. In practice, Respondent had no customer identification program for

DVP accounts during the period covered by the allegations in the Complaint because it believed there was a very low risk to the firm of money laundering through DVP accounts. Tr. 610 – 611.

There is no exclusion from the customer identification requirements for DVP accounts. In fact, there is authority supporting the application of customer identification requirements to DVP accounts. When the customer identification requirement went into effect for broker-dealers, some commenters on the proposed regulation suggested the exclusion of DVP accounts from the customer identification requirements. The final rule was implemented without the suggested change.[44]

Even before the AML requirements for broker-dealers went into effect, the Securities Industry Association advised the industry that accounts could not be excluded from AML review because of low risk: "[W]ith respect to institutional accounts, due diligence may need to be performed, notwithstanding the fact that these accounts do not represent a credit risk to the firm due to the delivery versus payment ('DVP') nature of the accounts."[45]

Respondent failed to follow both its own AML procedures, and the requirements of the Patriot Act and its implementing regulations, by failing to apply its customer identification procedures to DVP accounts. Because of this failure, Respondent's AML procedures were deficient for the period July 1, 2006, through April 20, 2007, thereby violating NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41.

V. SANCTIONS

There is no Sanction Guideline directly applicable to violations of NASD Conduct Rule 3011. In deciding on the appropriate sanctions, the Hearing Panel considered the Sanction

---

[44] FinCEN, Customer Identification Programs for Broker-Dealers, 68 Fed. Reg. 25113 (May 9, 2003); *see also Hartsfield Capital Securities, Inc.*, FinCEN, No. 2003-05, at n.4 (Nov. 24, 2003) (consent) (available on FinCEN website, www.fincen.gov).

[45] SIA, "Preliminary Guidance for Deterring Money Laundering Activity," at 8 – 9 (Feb. 13, 2002).

Guideline for deficient written supervisory procedures, as well as the General Principles Applicable to All Sanction Determinations and the Principal Considerations in Determining Sanctions. *FINRA Sanction Guidelines*, 2 – 7, 109 (2007). For deficient written supervisory procedures, the Sanction Guidelines recommend a fine of $1,000 to $25,000.

The Hearing Panel determined that the fines for the deficiencies in the 2006 and 2007 AML program should be determined individually, rather than determining an amount for one overall fine, because the considerations were somewhat different for each of the deficiencies. For Respondent's failure to identify certain foreign banks and obtain a certification for UBank, Next Century Investors, and the Bank of Montreal, the Hearing Panel finds that a fine of $5,000 is appropriate. Although the Hearing Panel found that Respondent's procedures overall were adequate, foreign financial institutions may pose a particular money laundering risk, so a fine is appropriate for Respondent's failure to identify certain foreign banks and to obtain the certifications.

For Respondent's failure to have written procedures to comply with Section 312, the Hearing Panel finds that a fine of $10,000 is appropriate. In reaching this conclusion, the Hearing Panel considered the fact that the requirement has been in place since 2002, it was explicitly discussed in NTM 02-21, and Respondent had no procedures at all for complying with this statutory requirement.

The Hearing Panel considers Respondent's failure to follow its own customer identification procedures for DVP accounts to be the most serious deficiency in its AML procedures for 2006 and 2007. Respondent's own procedures required customer identification procedures to be followed for DVP accounts, and it was required by the Patriot Act. Respondent's attempt to justify the omission by arguing that the risk to the firm was small is not

a reasonable position. Respondent cannot substitute its risk assessment for the assessments of Congress and FinCEN. The Hearing Panel finds that a fine of $25,000 is appropriate for this deficiency.

In total, the Hearing Panel finds that the appropriate sanction for the deficiencies in Respondent's AML program during 2006 and 2007 is a fine of $40,000.

VI. Conclusion

Respondent violated NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41, by failing to implement an adequate AML program for 2006 and 2007. For these violations, Respondent is fined $40,000.

Respondent is ordered to pay the costs of the hearing in the amount of $5,645.20, which includes a $750 administrative fee and the cost of the hearing transcript. The fine and costs shall be payable on a date set by FINRA, but not less than 30 days after this Decision becomes FINRA's final disciplinary action in this matter.

HEARING PANEL.

____
Lawrence B. Bernard
Hearing Officer

Copies to:
Sterne, Agee & Leach, Inc. (*via overnight courier and first-class mail*)
Gerald J. Russello, Esq. (*via e-mail and first-class mail*)
Paul M. Tyrrell, Esq. (*via e-mail and first-class mail*)
Laura Leigh Blackston, Esq. (*via e-mail and first-class mail*)
Karen E. Whitaker, Esq. (*via e-mail and first-class mail*)
Mark P. Dauer, Esq. (*via e-mail*)
David R. Sonnenberg, Esq. (*via e-mail*)