FINANCIAL SERVICES WEEKLY NEWS ROUNDUP

ASSESSMENTS OF CIVIL MONEY PENALTY

FinCEN Steps Up Civil Assessments Against Individuals and Smaller Outfits

In re Thomas E. Haider ..... TAB 1

In Re North Dade Community Development Federal Credit Union Miami Gardens, Florida ..... TAB 2

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

IN THE MATTER OF:	**)**	
	)	**Number 2014-08**
Thomas E. Haider	**)**	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network ("FinCEN") has determined that Thomas E. Haider willfully violated the Bank Secrecy Act ("BSA") and its implementing regulations, and has concluded that grounds exist to assess a $1 million civil money penalty against Haider pursuant to that Act.[1] During the relevant period, Haider was the Chief Compliance Officer and Senior Vice President of Government Affairs at MoneyGram International Inc. ("MoneyGram").

FinCEN has authority to investigate financial institutions and their partners, directors, officers, and employees for violations of the BSA pursuant to 31 C.F.R. § 1010.810, which grants FinCEN "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter."

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5314, 5316-5332. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Chapter X.

II. DETERMINATIONS

FinCEN has conducted an investigation and has concluded that Haider willfully violated the BSA and its implementing regulations.[2] Specifically, and as described below, Haider (1) willfully violated the requirement to implement and maintain an effective anti-money laundering program, 31 U.S.C. §§ 5318(a)(2) and 5318(h); 31 C.F.R. § 1022.210; and (2) willfully violated the requirement to report suspicious activity, 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320.

A. Introduction

1. Since at least 2003, MoneyGram has operated a money transfer service that enables customers to transfer money from one location to another through a global network of agents and outlets. MoneyGram outlets are independently-owned entities (such as convenience stores and internet cafes) that are authorized to transfer money through MoneyGram's money transfer system. MoneyGram agents are the owners and/or operators of such outlets.

2. As a money transmitter, MoneyGram is subject to, and must comply with, various requirements set forth in the BSA and its implementing regulations. As relevant here, and at all times relevant to this Assessment, MoneyGram was required to implement and maintain an effective anti-money laundering ("AML") program. MoneyGram was also required to file with

[2] In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. *See United States v. Williams*, 489 Fed. Appx. 655, 658, 660 (4th Cir. 2012); *United States v. McBride*, 908 F. Supp. 2d 1186, 1204-05 (D. Utah 2012); *see generally Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 57-58 (2007) ("where willfulness is a statutory condition of civil liability, we have generally taken it to cover not only knowing violations of a standard, but reckless ones as well").

FinCEN suspicious activity reports ("SARs") identifying financial transactions that: (1) were sent by or through MoneyGram; (2) involved (individually or in the aggregate) funds of at least $2,000; and (3) MoneyGram knew, suspected, or had reason to suspect involved, among other things, the use of MoneyGram's money transfer system to facilitate criminal activity. Such SARs were required to be filed within 30 days of MoneyGram detecting facts that may have constituted a basis for filing the SARs.

3. MoneyGram's Chief Compliance Officer was responsible for ensuring that the Company implemented and maintained an effective AML program and complied with its SAR-filing obligations. From at least 2003 through on or about May 23, 2008, Haider was MoneyGram's Chief Compliance Officer. Haider's employment at MoneyGram ended on or about May 23, 2008.

4. Notwithstanding Haider's obligations as MoneyGram's Chief Compliance Officer, at all times relevant to this Assessment, Haider failed to ensure that MoneyGram (1) implemented and maintained an effective AML program and (2) fulfilled its obligation to file timely SARs. Haider's failures included the following:

- **Failure to Implement a Discipline Policy.** Haider failed to ensure that MoneyGram implemented a policy for disciplining agents and outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.

- **Failure to Terminate Known High-Risk Agents/Outlets.** Haider failed to ensure that MoneyGram terminated agents and outlets that MoneyGram personnel understood were involved in fraud and/or money laundering, including outlets that Haider himself was on notice posed an unreasonable risk of fraud and/or money laundering.

- **Failure to File Timely SARs.** Haider failed to ensure that MoneyGram fulfilled its obligation to file timely SARs, including because Haider maintained MoneyGram's AML program so that the individuals responsible for filing SARs were not provided with information possessed by MoneyGram's Fraud Department that should have resulted in the filing of SARs on specific agents or outlets.

- **Failure to Conduct Effective Audits of Agents/Outlets.** Haider failed to ensure that MoneyGram conducted effective audits of agents and outlets, including outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.

- **Failure to Conduct Adequate Due Diligence on Agents/Outlets.** Haider failed to ensure that MoneyGram conducted adequate due diligence on prospective agents, or existing agents seeking to open additional outlets, which resulted in, among other things, MoneyGram (1) granting outlets to agents who had previously been terminated by other money transmission companies and (2) granting additional outlets to agents who MoneyGram personnel knew or suspected were involved in fraud and/or money laundering.

5. As a result of Haider's above-described AML failures, agents and outlets that MoneyGram personnel knew or suspected were involved in fraud and/or money laundering were allowed to continue to use MoneyGram's money transfer system to facilitate their fraudulent schemes. Haider's above-referenced failures continued throughout the time period relevant to this Assessment, and resulted in MoneyGram's customers suffering substantial losses (as many were duped into using MoneyGram's money transfer system to send significant sums of money to perpetrators of fraudulent schemes).

6. Under the BSA and its implementing regulations, individuals responsible for a company's failure to implement and maintain an effective AML program are liable for a civil money penalty of $25,000 for each day that the company lacks an effective AML program. Similarly, individuals responsible for a company's failure to file required SARs are liable for a civil money penalty of no less than $25,000 (and up to $100,000) for each instance in which the company fails to file a required SAR. Finally, FinCEN may seek injunctive relief against such individuals to (1) enforce compliance with the BSA and its implementing regulations and (2) protect the public from future harm.

7. Haider is a former employee and officer of MoneyGram, a global money services business currently headquartered in Dallas, Texas. At all times relevant to this Assessment,

MoneyGram provided the public with, among other services, money transmission services. As such, MoneyGram was a "financial institution," a "money services business," and a "money transmitter" within the meaning of the BSA and its implementing regulations. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 103.11(n)(3), (uu), *re-codified in 2011 at* 31 C.F.R. § 1010.100(t)(3), (ff).[3]

8. At all times relevant to this Assessment, Haider served as MoneyGram's Chief Compliance Officer, supervising both MoneyGram's Fraud and AML Compliance Departments.

B. Background

1. The Relevant Statutory and Regulatory Provisions of the Bank Secrecy Act

9. As set forth below, the BSA and its implementing regulations require, among other things, that financial institutions: (1) implement an effective AML program to prevent the financial institutions from being used to facilitate money laundering or the financing of terrorist activities; and (2) report suspicious transactions involving potentially unlawful activity. *See* 31 U.S.C. § 5318(g), (h); 31 C.F.R. §§ 103.20, 103.125, *re-codified at* 31 C.F.R. §§ 1022.320, 1022.210.

10. FinCEN is a bureau within the Department of the Treasury. The Secretary of the Department of the Treasury has delegated to the Director of FinCEN the authority to implement and enforce compliance with the BSA, including through the promulgation of regulations. *See* 31 U.S.C. § 310(b)(2)(I); Treasury Order 180-01.

[3] Prior to 2011, the BSA regulations relevant to this Assessment were codified at 31 C.F.R. Part 103. In 2011, those regulations were re-codified at 31 C.F.R. Chapter X. Because the conduct relevant to this Assessment occurred prior to 2011, this Assessment cites to 31 C.F.R. Part 103 with references to the updated citations.

a. The Requirement to Implement an Effective AML Program

11. The BSA requires that all financial institutions establish an AML program that "includ[es], at a minimum": (1) "the development of internal policies, procedures, and controls"; (2) "the designation of a compliance officer"; (3) "an ongoing employee training program"; and (4) "an independent audit function to test [the] program[]." 31 U.S.C. § 5318(h)(1).

12. In 2002, FinCEN issued a regulation implementing 31 U.S.C. § 5318(h)(1). *See* 31 C.F.R. § 103.125, *re-codified at* 31 C.F.R. § 1022.210. That regulation (which was in effect at all times relevant to this Assessment) requires that all money services businesses ("MSBs"), including those that function as money transmitters (like MoneyGram), "develop, implement, and maintain an effective [AML] program." *Id.* § 103.125(a), *re-codified at* 31 C.F.R. § 1022.210(a). The regulation provides that "[a]n effective [AML] program is one that is reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities," and "shall be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the [MSB]." *Id.* § 103.125(a)-(b), *re-codified at* 31 C.F.R. § 1022.210(a)-(b).

13. The above-referenced regulation, 31 C.F.R. § 103.125, (*re-codified at* 31 C.F.R. § 1022.210), also provides that an effective AML program must, "[a]t a minimum": (1) "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance with [the requirements of 31 C.F.R. Part 103]," including policies for the "[f]iling [of] reports"; (2) "[d]esignate a person to assure day to day compliance with the [AML] program and [the requirements of 31 C.F.R. Part 103]" (the "AML Compliance Officer"); (3) "[p]rovide education and/or training [to] appropriate personnel concerning their responsibilities under the [AML] program, including training in the detection of suspicious transactions to the extent that

the [MSB] is required to report such transactions under [31 C.F.R. Part 103]"; and (4) "[p]rovide for independent review to monitor and maintain an adequate [AML] program." *Id.* § 103.125(d)(1)-(4), *re-codified at* 31 C.F.R. § 1022.210(d)(1)-(4).

14. Pursuant to 31 C.F.R. § 103.125, (*re-codified* at 31 C.F.R. § 1022.210), an MSB's AML Compliance Officer must, among other things, ensure that: (1) "[t]he [MSB] properly files reports . . . in accordance with applicable requirements of [31 C.F.R. Part 103]"; (2) "[t]he [MSB's] compliance program is updated as necessary to reflect current requirements of [31 C.F.R. Part 103], and related guidance issued by the Department of the Treasury"; and (3) "[t]he [MSB] provides appropriate training and education in accordance with [31 C.F.R. § 103.125(d)(3)]." *Id.* § 103.125(d)(2), *re-codified at* 31 C.F.R. § 1022.210(d)(2).

15. In late 2004, FinCEN issued "Interpretive Release 2004-01" (the "2004 Interpretive Release"), through which it clarified that, pursuant to 31 C.F.R. § 103.125 (*re-codified* at 31 C.F.R. § 1022.210), MSBs that do business through agents or counterparties located outside of the United States (like MoneyGram) must implement and maintain as part of their AML program risk-based policies, procedures, and controls designed to identify and minimize money laundering and terrorist financing risks associated with such foreign agents and counterparties.

16. In the 2004 Interpretive Release, FinCEN stated that "[t]o the extent [MSBs] utilize relationships with foreign agents or counterparties to facilitate the movement of funds into or out of the United States, they must take reasonable steps to guard against the flow of illicit funds, or the flow of funds from legitimate sources to persons seeking to use those funds for illicit purposes, through such relationships." Accordingly, FinCEN made clear that such MSBs' AML programs should, among other things: (1) "establish procedures for conducting

reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the [MSBs'] products and services," including "reasonable procedures . . . to evaluate, on an ongoing basis, the operations of those foreign agents and counterparties"; (2) "establish procedures for risk-based monitoring and review of transactions from, to, or through the United States that are conducted through foreign agents and counterparties" sufficient to "enable the [MSBs] to identify and, where appropriate, report as suspicious such occurrences as[] instances of unusual wire activity"; and (3) "[establish] procedures for responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism," including procedures that "provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that [an MSB] determines poses an unacceptable risk of money laundering . . . ."

17. The 2004 Interpretive Release identified a number of "[r]elevant risk factors" that an MSB should consider in evaluating a foreign agent or counterparty, including "[a]ny information known or readily available to the [MSB] about the foreign agent or counterparty's [AML] record" and "[t]he types and purpose of services to be provided to, and anticipated activity with, the foreign agent or counterparty." *See also Matter of Western Union Fin. Servs., Inc.*, No. 2003-2 (Mar. 6, 2003) (indicating that MSBs that do business through agents or counterparties located within the United States are subject to similar requirements).

b. The Requirement to Report Suspicious Activity

18. The BSA also authorizes FinCEN to "require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1).

19. In 2000, FinCEN issued a regulation implementing 31 U.S.C. § 5318(g)(1). *See* 31 C.F.R. § 103.20, *re-codified at* 31 C.F.R. § 1022.320. That regulation (which was amended in relevant part in 2003 and in effect at all times relevant to this Assessment) requires that certain MSBs, including ones that function as money transmitters (like MoneyGram), report any "transaction . . . [that] is conducted or attempted by, at, or through [the MSB], involves or aggregates funds or other assets of at least $2,000 . . . , and the [MSB] knows, suspects, or has reason to suspect":

- "[i]nvolves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity . . . as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation";

- "[i]s designed, whether through structuring or other means, to evade any requirements of [31 C.F.R. Part 103] or of any other regulations promulgated under the [BSA]";

- "[s]erves no business or apparent lawful purpose, and the reporting [MSB] knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction"; or

- "[i]nvolves use of the [MSB] to facilitate criminal activity."

Id. § 103.20(a)(1)-(2), *re-codified at* 31 C.F.R. § 1022.320(a)(1)-(2). At all times relevant to this Assessment, MSBs were required to report such transactions by filing a SAR "no later than 30 calendar days after the date of the initial detection by the [MSB] of facts that may constitute a basis for filing a SAR[]." *Id.* § 103.20(b)(3), *re-codified at* 31 C.F.R. § 1022.320(b)(3).

20. At all times relevant to this Assessment, FinCEN required SARs to be filed on a standard form. That form was divided into multiple sections, with the following titles and purposes: (1) "Subject Information," wherein the reporting party was to identify the suspected wrongdoer and indicate whether that individual or entity was the "[p]urchaser/sender" or "[p]ayee/receiver," or had some other role in the suspicious transaction(s); (2) "Suspicious Activity Information," wherein the reporting party was to provide specific details regarding the suspicious activity, including its date or date range; (3) "Transaction Location," wherein the reporting party was to identify the physical location where the suspicious activity had occurred, and identify whether it was the "[s]elling location," the "[p]aying location," or some other location; (4) "Reporting Business" and "Contact for Assistance," wherein the reporting party was to provide certain information about itself; and (5) "Suspicious Activity Information – Narrative," wherein the reporting party was to provide a narrative description of the subject's suspicious activity. *See* FinCEN Form 109; Form TD F 90-22.56.

c. Enforcement of the BSA and Its Implementing Regulations

21. Under the BSA, any domestic financial institution — or any "partner, director, officer, or employee" of any such institution — that "willfully" violates the BSA or its implementing regulations is liable "for a civil penalty of not more than the greater of the amount (not to exceed $100,000) involved in the transaction (if any) or $25,000." 31 U.S.C. § 5321(a)(1). For violations of a financial institution's duty to implement an effective AML program, "a separate violation occurs for each day the violation continues and at each office, branch, or place of business at which a violation occurs or continues." *See id.*

C. MoneyGram's Money Transfer Business

22. At all times relevant to this Assessment, MoneyGram operated a money transfer service that enabled customers to transfer money to and from various locations in the United States and abroad through MoneyGram's global network of agents and outlets.

23. MoneyGram outlets were independently-owned entities that MoneyGram authorized to transfer money through its money transfer system. Typically, MoneyGram outlets were businesses (such as convenience stores and internet cafes) that offered money transfers through MoneyGram, but primarily provided other types of goods and services.

24. MoneyGram agents were individuals or entities that owned and/or operated MoneyGram outlets.

25. MoneyGram had the right to terminate its agents/outlets for a variety of reasons, including suspected involvement in fraud or money laundering.

26. To send money using MoneyGram's money transfer system, customers went to a MoneyGram outlet and completed a "send" form, on which they identified the name of the recipient and the state or province and country where the money was to be sent. The MoneyGram agent then collected the money to be transferred plus a fee from the customer and entered the information from the send form into a transaction database maintained by MoneyGram.

27. To receive a MoneyGram money transfer, the payee was required to physically appear at a MoneyGram outlet and complete a "receive" form. On the receive form, the payee listed, among other things, his or her name and the expected transfer amount. The MoneyGram agent at the receive location then queried MoneyGram's transaction database to find the money

transfer intended for the payee. Upon locating the money transfer, the agent paid the payee. The payee was paid either in cash or in the form of a MoneyGram transfer check or money order.

28. MoneyGram profited from its money transfer business by collecting a fee from each send transaction processed by one of its agents/outlets. Accordingly, to maximize profits, MoneyGram had an incentive to expand the number of its agents/outlets, and it had a disincentive to terminate agents/outlets.

29. MoneyGram maintained thousands of agents and outlets throughout the United States.

D. MoneyGram's Internal Organizational Structure

30. At all times relevant to this Assessment, MoneyGram was organized by department, with different departments having responsibilities for different functions. The departments included (1) Fraud, (2) AML Compliance, (3) Risk, and (4) Sales.

31. The Fraud Department was responsible for, among other things, identifying existing agents/outlets that might be engaging in fraud against MoneyGram or its customers, and investigating such agents/outlets to determine whether action should be taken against them.

32. The AML Compliance Department was responsible for, among other things, the day-to-day operations of MoneyGram's AML program, including (1) evaluating prospective agents/outlets, (2) auditing existing agents/outlets, and (3) formulating policies to ensure that SARs were filed in accordance with the BSA and its implementing regulations.

33. The Risk Department was responsible for, among other things, identifying existing agents/outlets that posed a heightened risk to the Company, and investigating such agents/outlets to determine whether action should be taken against them.

34. The Sales Department was responsible for, among other things, developing relationships with potential agents/outlets, and maintaining MoneyGram's relationships with existing agents/outlets.

35. MoneyGram also had a call center that, among other things, fielded complaints from MoneyGram customers from around the world who called to report that they had been the victims of fraud (*i.e.*, they had been induced by fraud to send money transfers using MoneyGram's money transfer system). These complaints were memorialized in Consumer Fraud Reports. Each Consumer Fraud Report included, among other things, the identity of the defrauded consumer, the name of the MoneyGram outlet that had sent the fraudulent money transfer, and the name of the MoneyGram outlet that had received the fraudulent money transfer. The call center forwarded the Consumer Fraud Reports to MoneyGram's Fraud Department for investigation. When this Assessment refers to the number of Consumer Fraud Reports accumulated by a particular outlet during a specified time period, it is referring to the number of Consumer Fraud Reports received by MoneyGram during that time period identifying the outlet as the receiving outlet for fraud-induced money transfer.

E. Haider's Role Within MoneyGram

36. As set forth above, at all times relevant to this Assessment, Haider was MoneyGram's Chief Compliance Officer and supervised the AML Compliance Department. Haider also supervised MoneyGram's Fraud Department. MoneyGram's "Senior Director of AML Compliance," "Director of AML Compliance and Fraud," and "Director of Fraud" all worked under, and had direct contact with, Haider.

37. As MoneyGram's Chief Compliance Officer, Haider was responsible for ensuring that MoneyGram complied with its obligations under the BSA and its implementing regulations,

including that it (1) implemented and maintained an effective AML program, and (2) complied with its SAR-reporting obligations.

38. Haider was the architect of MoneyGram's AML program, and was also responsible for assuring the Company's day-to-day compliance with it and for approving AML-related policy changes as appropriate. In addition, Haider was responsible for ensuring that MoneyGram's AML program complied with the requirements of the BSA and its implementing regulations.

39. As MoneyGram's Chief Compliance Officer, Haider had the authority to terminate or otherwise discipline MoneyGram agents and outlets because of compliance concerns. Haider also had the authority to decline to approve new agents/outlets.

40. Notably, after leaving MoneyGram in 2008, Haider stated that he did not recall anyone exerting any undue pressure on him not to terminate an agent that he wanted to terminate.

41. Beginning in 2006, and continuing throughout the remainder of his employment at MoneyGram, Haider was a member of MoneyGram's Senior Leadership Team, an executive management group whose members reported directly to MoneyGram's Chief Executive Officer ("CEO").

42. Although Haider did not report directly to MoneyGram's Board of Directors (the "Board"), he made presentations quarterly to the Audit Committee of the Board to keep the Board apprised of developments in the AML program. In addition, there was an open line of communication between Haider and the Audit Committee, and Haider's reports to the Audit Committee were not screened by MoneyGram's other senior managers.

43. Haider received an annual salary from MoneyGram, as well as an annual bonus that was based in whole or part on the performance of the Company.

F. Fraudulent Use of MoneyGram's Money Transfer Business

44. From as early as 2003, and continuing throughout Haider's employment at MoneyGram, certain MoneyGram agents and outlets located in the United States and Canada participated in schemes to defraud the public, using MoneyGram's money transfer system to facilitate the schemes.

45. The fraudulent schemes relied on a variety of false promises and other representations aimed at misleading the public and inducing unsuspecting victims to send money through MoneyGram's money transfer system, using the participating MoneyGram agents and outlets. The participating MoneyGram agents and outlets, together with other co-conspirators (collectively, the "perpetrators"), solicited victims through the mail, internet, and telephone, telling the victims, among other things, that they had won a lottery, had been hired for a "secret shoppers" program through which they would be paid to evaluate retail stores, had been approved for a guaranteed loan, or had been selected to receive an expensive item or cash prize. The victims were told that to receive the item or benefit, they had to pay the perpetrators some amount of money in advance. For example, in situations where the victims were promised lottery winnings or cash prizes, they were told that they had to pay taxes, customs' duties, or processing fees up front. The victims were directed to send the advance payments to fictitious payees using MoneyGram's money transfer system.

46. After such payments had been sent, the agents participating in the fraud on the receiving end would remove the victims' money from MoneyGram's money transfer system and the money would ultimately be divided among the perpetrators. In some instances, the

participating agents on the receiving end would further transfer the victims' money to additional participants in the scheme before the money was divided among the perpetrators. In other instances, participating agents would identify fraudulent money transfers in MoneyGram's money transfer system and then instruct other participating agents to remove the victims' money from the money transfer system. These additional steps were designed to conceal the ultimate destination of the fraud proceeds by "laundering" the victims' money.

47. Some of the MoneyGram agents involved in the above-referenced fraudulent schemes have since been charged criminally and convicted, and are now serving prison terms.

G. MoneyGram's Prior Resolutions with the Federal Trade Commission and the Department of Justice

48. On October 19, 2009, the Federal Trade Commission ("FTC") filed a complaint against MoneyGram, alleging that from 2004 through 2008, MoneyGram agents in the United States and Canada aided fraudulent telemarketers and other perpetrators of telephone and internet scams who misled U.S. consumers into wiring tens of millions of dollars to participants in the fraud. In October 2009, MoneyGram settled the FTC's consumer fraud claims by agreeing to pay an assessed penalty of $18 million.

49. On November 9, 2012, MoneyGram entered into a Deferred Prosecution Agreement ("DPA") with the Department of Justice's Asset Forfeiture and Money Laundering Section and the U.S. Attorney's Office for the Middle District of Pennsylvania ("MDPA") on charges of aiding and abetting wire fraud, in violation of 18 U.S.C. §§ 1343 and 2, and willfully failing to implement an effective AML program, in violation of 31 U.S.C. § 5318(h). MoneyGram agreed to forfeit $100 million as part of the DPA and to retain an independent compliance monitor approved by the Department of Justice.

50. As part of the DPA, MoneyGram admitted, among other things, that it had "willfully failed to maintain an effective [AML] program that was reasonably designed to prevent it from being used to facilitate money laundering." *United States v. MoneyGram Int'l, Inc.*, 12-cr-291 (M.D. Pa. 2012), Docket 3-1, at ¶ 31. The specific programmatic failures to which MoneyGram admitted included:

- "MoneyGram failed to implement policies or procedures governing the termination of Agents involved in fraud and money laundering."

- "MoneyGram failed to implement policies or procedures to file the required SARs when victims reported fraud to MoneyGram on transactions over $2,000. Instead, MoneyGram structured its AML program so that individuals responsible for filing SARs did not have access to the Fraud Department's Consumer Fraud Report database."

- "MoneyGram filed [SARs], in which [it] incorrectly listed the victim of the fraud as the individual who was the likely wrongdoer. MoneyGram failed to file SARs on their Agents who MoneyGram knew were involved in the fraud."

- "MoneyGram failed to conduct effective AML audits of its Agents and Outlets. MoneyGram's Senior Director of Anti-Money Laundering refused to conduct audits on certain Outlets involved in fraud and money laundering that MoneyGram refused to terminate because the Outlets were 'criminal operations' and sending their audit team into those Outlets would put the audit team in 'physical danger.'"

- "MoneyGram failed to implement policies or procedures to review MoneyGram transfer checks of Agents known or suspected to be involved in 'check pooling,'" a type of money-laundering scheme.

- "MoneyGram failed to conduct adequate due diligence on prospective MoneyGram Agents. MoneyGram routinely signed up new Agents without visiting the locations or verifying that a legitimate business existed. As a result, some of the Agents involved in fraud and money laundering operated out of homes in residential neighborhoods and other locations that were not open to the public."

- "MoneyGram failed to conduct adequate due diligence on MoneyGram Agents seeking additional MoneyGram Outlets. MoneyGram routinely granted additional Outlets to Agents known to be involved in fraud and money laundering."

Id. The above programmatic failures all existed while Haider was MoneyGram's Chief Compliance Officer, and resulted in MoneyGram violating the BSA.

H. Haider Willfully Failed to Ensure that MoneyGram Implemented and Maintained an Effective AML Program

1. Haider Failed to Implement a Policy for Disciplining Agents/Outlets, or to Terminate Agents/Outlets that He Knew or Should Have Known Posed an Unreasonable Risk of Fraud and Money Laundering

a. Haider Failed to Implement a Policy for Disciplining Agents/Outlets

51. Throughout Haider's tenure as MoneyGram's Chief Compliance Officer, he failed to implement a policy for terminating or otherwise disciplining agents/outlets that presented a high risk of fraud and money laundering.

52. Moreover, while Haider was in charge of MoneyGram's compliance program, MoneyGram rejected or ignored at least two written discipline policies — proposed by the Fraud Department — that would have required that outlets be terminated or otherwise disciplined if, within a defined period, they accumulated a certain number of Consumer Fraud Reports or reached a certain dollar amount of consumer fraud payouts. For example, in 2006, the Fraud Department proposed a policy to terminate or otherwise discipline "suspect Canadian locations." Under this policy, an outlet would have been terminated if it accumulated 15 Consumer Fraud Reports or $22,500 in fraud payouts within three months, 20 Consumer Fraud Reports or $30,000 in fraud payouts within six months, or 25-30 Consumer Fraud Reports or $37,500-$45,000 in fraud payouts within one year. The proposed policy provided for lesser discipline (*i.e.*, a warning letter or phone call) if an outlet met lesser benchmarks during the defined periods.

53. In March 2007, the Fraud Department proposed a similar policy that would have been applicable to all outlets, not just those located in Canada.

54. At a minimum, the March 2007 policy was presented to Haider. Yet Haider not only failed to implement it, but also failed to implement any policy for terminating or otherwise disciplining high-risk agents/outlets during his employment at MoneyGram.

55. Haider's failure to ensure that a discipline policy was implemented was particularly egregious given that: (1) in an April 17, 2007 letter, MoneyGram's outside counsel told the FTC that, "[d]ue to MoneyGram's concern about [certain Canadian outlets], MoneyGram . . . plans to institute a new policy to review fraud activity at the individual agent level on a quarterly basis, looking specifically at the number of reported fraud transactions and dollar value of those transactions in particular time frames. The policy will also include criteria for the trigger points for sending warning letters to agents, agent suspensions, and agent terminations"; (2) in or about 2007, MoneyGram provided its external AML consultant with a proposed set of guidelines to govern the termination of agents; and, as set forth below in Part H.1.b, (3) Haider was on notice that numerous MoneyGram agents/outlets presented a high risk of fraud and money laundering.

56. Additionally, in mid-August 2007, MoneyGram's then Director of Fraud created a powerpoint presentation, titled "High Fraud Agents," in which, among other things, he: (1) observed that MoneyGram "does not have a consistent repeatable process to restrict agents that receive a disproportionate amount of fraudulent wire transfers (high fraud agents)"; (2) stated that "[w]e need to implement an on-going plan to address High Fraud Agents"; and (3) expressly "[r]ecommend[ed] implementing [a] Fraud Agent Closure Policy." The presentation concluded by identifying several "next steps," including "[r]eview [r]ecommendations w/Tom H. (8/21)" and "[i]mplement [p]olicy 9/17/07." Nevertheless, no discipline policy was implemented by MoneyGram prior to Haider leaving the Company.

57. Haider had the authority to implement a discipline policy. Therefore, to the extent the Sales Department or others successfully resisted implementation of such a policy, Haider allowed it to happen.

58. Haider's failure to implement a discipline policy allowed numerous agents/outlets that MoneyGram personnel knew or suspected were defrauding consumers, and that therefore presented an unreasonable risk of money laundering, to continue using MoneyGram's money transfer system to facilitate their fraudulent schemes.

b. Haider Failed to Terminate Agents/Outlets that He Knew or Should Have Known Posed an Unreasonable Risk of Fraud and Money Laundering

59. From approximately January 2004 through May 2008, MoneyGram customers filed with MoneyGram more than 30,000 Consumer Fraud Reports involving MoneyGram agents/outlets in the United States and Canada, totaling approximately $60 million in consumer losses. Many of these customers were residents of the United States who reported being defrauded into sending money transfers that were received by MoneyGram agents/outlets in Canada. Indeed, most Consumer Fraud Reports involved money transfers that were sent from the United States and received either in Canada or the United States. Notably, the actual number of defrauded consumers and loss amount was higher than the figures presented above, because, as MoneyGram personnel recognized, not all victims of fraud reported the fraud to MoneyGram.

60. Beginning as early as 2003, and continuing throughout Haider's employment at MoneyGram, MoneyGram's Fraud Department compiled data from the Consumer Fraud Reports in an electronic fraud database (the "Consumer Fraud Report database"). That database was used to create reports identifying, among other things, the number of fraud complaints received in connection with specific MoneyGram outlets during specified time periods.

i. Haider Received Data From the Consumer Fraud Report Database Identifying High-Risk Agents/Outlets, and Failed to Terminate Them

61. Haider knew of the Consumer Fraud Report database, and received information and reports from it. For example, in March 2007, Haider received spreadsheets identifying specific outlets that had accumulated an alarmingly high number of Consumer Fraud Reports. One such spreadsheet, which Haider received on or about March 15, 2007, was titled "2006: Locations in Canada that Have Received Fraud Induced Money Transfers — Percentages of Fraud Induced Transfers." That spreadsheet, which listed all of the Canadian outlets that had received at least one fraud-induced money transfer in 2006, revealed that the top 10 outlets in terms of losses to consumers had received between 62 and 241 fraud-induced money transfers in 2006 alone, resulting in losses to consumers of between $171,946.00 and $419,838.30. For those 10 outlets, an exceedingly high percentage of their total number of received money transfers in 2006 were reported as fraudulent: between 8.7% and 16.2%. Moreover, eight of the 10 outlets appeared on another spreadsheet that Haider received on or about March 15, 2007, which contained analogous data for 2005. For those eight outlets, a high percentage of their total number of received money transfers in 2005 were also reported as fraudulent: between 7.8% and 25.3%. Of the above-referenced 10 outlets, only one was terminated by MoneyGram during Haider's employment at the Company. The remaining nine outlets were terminated within one year of Haider leaving MoneyGram.[4] Most or all of the above outlets had the vast majority of their received money transfers originate from consumers located in the United States.

[4] One of those nine outlets, while still affiliated with MoneyGram at the time Haider left the Company, appears to have stopped sending or receiving money transfers as of August 18, 2007 (*i.e.*, prior to Haider leaving MoneyGram, but no less than five months after Haider was put on notice of the outlet's high-risk status).

ii. Haider Received Recommendations to Terminate Specific Agents/Outlets Supported By Data from the Consumer Fraud Report Database, and Failed to Terminate Them

62. Haider also received periodic recommendations from the Fraud Department to terminate specific agents and outlets for fraud. Those recommendations were supported by data from the Consumer Fraud Report database, and primarily involved fraudulent money transfers that originated from U.S. customers.

a) The April 2007 Spreadsheets

63. In late March or early April 2007 — after MoneyGram had received a subpoena from the FTC in January 2007 seeking data regarding its Canadian outlets, including the percentage of their received money transfers that were reported as fraudulent — MoneyGram's then Director of AML Compliance and Fraud compiled a list of approximately 30 outlets in Canada that the Fraud Department was recommending be terminated for fraud. MoneyGram's then Senior Director of AML Compliance has since described those outlets as "the worst of the worst," with levels of fraud complaints that were "egregious and beyond anyone's ability to doubt that the agent had knowledge and involvement."

64. Thereafter, on April 20, 2007, the Director of AML Compliance and Fraud emailed Haider and other senior managers two spreadsheets (the "April 2007 Spreadsheets") listing 49 Canadian outlets that the Fraud Department was proposing for termination. The April 2007 Spreadsheets included approximately 30 outlets that the Fraud Department had previously recommended for termination, plus additional outlets that it was also recommending be terminated or at least sent warning letters and then very closely monitored. The April 2007 Spreadsheets contained information indicating that the 49 outlets were either engaging in or turning a blind eye to fraud, including data from the Consumer Fraud Report database showing

that most of the outlets: (1) had an excessively high number of received money transfers reported as fraudulent; (2) had an excessively high percentage of their total number of received money transfers reported as fraudulent; (3) had an excessively high percentage of their received money transfers originate from the United States; and/or (4) received more money transfers than they sent.

65. Officials within the Fraud and AML Compliance Departments viewed the above characteristics as indicators of fraud. MoneyGram outlets in developed countries like the United States and Canada typically send (1) money transfers to less-developed countries, and (2) more money transfers than they receive. Therefore, it was unusual to see outlets in Canada receiving (1) significant numbers of money transfers from the United States, or (2) more money transfers than they sent. Moreover, most MoneyGram outlets did not accumulate any Consumer Fraud Reports. Therefore, it was unusual for an outlet to have more than a few (or more than 1% or 2%) of its received transactions reported as fraudulent.

66. In addition to the information described above, the April 2007 Spreadsheets conveyed the following specific information about the 49 outlets:

- During the six-month period from September 2006 through February 2007 (the "six-month period"), the 49 outlets accounted for approximately 58% of all reported fraud involving money sent through MoneyGram's money transfer system to Canada.

- Twenty-three of the 49 outlets had accumulated at least 25 and as many as 106 Consumer Fraud Reports during the six-month period (the "highest fraud outlets"). In other words, during the six-month period, the 23 highest fraud outlets had received between 25 and 106 fraud-induced money transfers.

- For those 23 highest fraud outlets, the fraudulent money transfers represented between 4.5% and 20.4% of their total number of received money transfers during the six-month period. Moreover, 21 of those 23 outlets had between 6.5% and 20.4% of their total number of received money transfers reported as fraudulent during the six-month period. Most of the other 49 outlets also had a high percentage of their total number of received money transfers reported as fraudulent during the six-month period; 23 had between 4.3% and 28.5%, while 19 had between 6.5% and 28.5%.

- During the six-month period, the 23 highest fraud outlets received between 75.9% and 100% of their total number of received money transfers from the United States. Seventeen of those outlets received more than 90% of their total number of received money transfers from the United States. Most of the other 49 outlets also received an exceedingly high percentage of their received money transfers from the United States, with 22 receiving 75% or more, 18 receiving 85% or more, and 13 receiving 90% or more.

- Many of the 49 outlets also received significantly more money transfers than they sent. For example, during the six-month period, 10 of those outlets had the following receive/send ratios: (1) 917 received/322 sent; (2) 267 received/24 sent; (3) 394 received/66 sent; (4) 426 received/153 sent; (5) 164 received/25 sent; (6) 522 received/169 sent; (7) 146 received/41 sent; (8) 179 received/38 sent; (9) 186 received/63 sent; and (10) 252 received/84 sent.

- For the broader group of 49 outlets, the fraudulent money transfers resulted in more than $3 million in consumer losses during the six-month period. For the 23 highest fraud outlets, the fraudulent transfers resulted in more than $2 million in consumer losses during the six-month period.

67. The April 2007 Spreadsheets also reflected that many of the 49 outlets had had a high percentage of their total number of received money transfers reported as fraudulent in prior years. For example, 10 of the outlets had the following percentages of their received money transfers reported as fraudulent during calendar years 2005 and 2006, respectively: (1) 13.1% and 12.2%; (2) 12.0% and 16.2%; (3) 13.5% and 11.2%; (4) 11.9% and 10.9%; (5) 25.3% and 11.0%; (6) 13.3% and 15.2%; (7) 18.6% and 12.1%; (8) 18.5% and 11.5%; (9) 9.1% and 14.6%; and (10) 15.3% and 11.6%.

68. During the above-referenced six-month period, the expected dollar value for legitimate money transfers from the United States to Canada was under $1,000. Therefore, officials within MoneyGram's Fraud and AML Compliance Departments considered an average dollar value for money transfers between the United States and Canada exceeding $1,000 as another indicator of fraud. The April 2007 Spreadsheets revealed that for many of the above-referenced 49 outlets, the average dollar value for their received money transfers exceeded

$1,000 and even $2,000. For example, for the 23 highest fraud outlets on the April 2007 Spreadsheets, 22 had an average dollar value for their received money transfers of at least $1,000, 17 had an average dollar value for their received money transfers of at least $1,500, and eight had an average dollar value for their received money transfers of at least $2,000.

b) Haider Failed to Terminate Most of the Outlets Identified On the April 2007 Spreadsheets

69. Despite the Fraud Department's proposal to terminate the above-referenced outlets, most of them remained affiliated with MoneyGram throughout Haider's employment at the Company. For example, of the broader group of 49 outlets identified on the April 2007 Spreadsheets: (1) only seven were terminated by MoneyGram during Haider's employment at the Company as a result of fraud; and (2) at least 33 were still affiliated with MoneyGram at the time Haider left the Company as a result of fraud.[5] Similarly, of the 23 highest fraud outlets: (1) only three were terminated by MoneyGram during Haider's employment at the Company; and (2) at least 18 were still affiliated with MoneyGram at the time of Haider's departure.[6] Notably, by August 2009, MoneyGram had terminated each of the above-referenced 33 outlets (of which the 23 highest fraud outlets were a subset). If Haider had implemented either of the discipline policies referenced above in paragraphs 52 and 53, 32 of those 33 outlets would have been terminated no later than April 2007.

70. Although MoneyGram placed a few of the 49 outlets referenced in the April 2007 Spreadsheets on "send only" status (meaning that they could send but not receive money

[5] Two of those 33 outlets, while still affiliated with MoneyGram at the time Haider left the Company, appear to have stopped sending or receiving money transfers as of June 25, 2007, and August 18, 2007, respectively. From May 1, 2007, through June 25, 2007, the first of those two outlets received approximately 95 fraud-induced money transfers, totaling more than $90,000 in consumer losses.

[6] One of those 18 outlets is the outlet referenced above that appears to have stopped sending or receiving money transfers as of June 25, 2007.

transfers), that response was clearly inadequate as to those unambiguously high-risk outlets. As early as 2005, senior officials within MoneyGram's Fraud Department recognized that placing such outlets on "send only" status was not sufficient. Indeed, by email dated February 2, 2005, the then Director of AML Compliance and Fraud (who also held that position in April 2007) wrote the following in response to a suggestion that a problem outlet be placed on "send only" status: "[P]lease be aware that we continue to see agents who are on send status surfing fraud transaction[s]. For example, I just found another situation where [an outlet that had been placed on 'send only' status] surfed a transaction that was then paid out at [another outlet]."[7] In another email from 2005 — this one dated December 8, 2005 — another Fraud Department employee resisted placing a problem outlet on "send only" status, stating, "We have tried restricting agents of concern to 'send' only in the past and that did not resolve the matter."

c) Four of the Non-Terminated Outlets were Owned and/or Operated by the Same Individual, and Were Involved in Money Laundering

71. Of the 49 outlets identified on the April 2007 Spreadsheets, four of them — Money Spot, Money Spot 2, Money Spot 5, and N&E Associates — were owned and/or operated by the same individual, James Ugoh. The April 2007 Spreadsheets reflected that, during the above-referenced six month period, those four outlets had collectively accumulated 150 Consumer Fraud Reports, totaling more than $300,000 in consumer losses. The April 2007 Spreadsheets also revealed that, during the six-month period, the four outlets accounted for 5.9% of all reported fraud involving money sent through MoneyGram's money transfer system to

[7] "Surfing" refers to the situation where one outlet — typically one that has been placed on "send only" status — uses MoneyGram's money transfer system to identify a fraud-induced money transfer for the purpose of contacting another outlet — which has not been placed on "send only" status — and directing that second outlet to "receive" the fraudulent money transfer and extract the fraudulently sent funds from MoneyGram's money transfer system.

Canada. Yet none of those outlets was terminated during Haider's employment at MoneyGram, notwithstanding that, as early as 2004, Haider was on notice that Money Spot was engaging in fraud. Indeed, in an email dated August 19, 2004, MoneyGram's then Director of AML Compliance and Fraud informed Haider that there was fraud occurring at Money Spot, and that the Toronto Police Department regarded Money Spot as "dirty." Specifically, the Director wrote to Haider:

> Hi Tom, I wondered if you had a chance to look over the report I gave you on Canada agents that we'd like to close due to high incidents of consumer fraud. We have also had surfing and wrong payouts at many of these agents. *We have had three more reports of cashiers check/internet fraud at Money Spot in Toronto. Toronto PD also called me — they think this agent is dirty.* We are anxious to move forward in closing all of most of [sic] these agents . . . .

(Emphasis added).

72. In the above-referenced DPA, MoneyGram admitted that, beginning in 2006 and continuing into early 2009, Ugoh — the above-referenced owner and/or operator of multiple MoneyGram outlets, including four that were included on the April 2007 Spreadsheets — conspired with other MoneyGram agents in the Toronto area in an extensive money laundering scheme to conceal the identities of the recipients of proceeds from consumer fraud schemes. Complicit MoneyGram agents in Canada received the initial fraudulent transaction from the victim via MoneyGram's money transfer system. The complicit MoneyGram agents then executed their money laundering scheme by making MoneyGram transfer checks payable to one of a few individuals responsible for laundering the money, instead of the fictitious payee to whom the victim believed the money was being sent. The checks were then collected and deposited into business accounts controlled by the individuals laundering the money. This practice, known as "check pooling," allowed Ugoh and others to deposit the checks into what

appeared to be legitimate bank accounts, and then ultimately withdraw and distribute the proceeds among the perpetrators.

73. Employees within MoneyGram's Fraud and AML Compliance Departments were on notice of the above-referenced check-pooling scheme — and of Ugoh's outlets' involvement in it — no later than January 2007. In January 2007, MoneyGram's then Director of AML Compliance and Fraud, as well as other members of MoneyGram's Fraud Department, received an email from an employee in MoneyGram's Agent Services Department indicating that multiple MoneyGram outlets, including Money Spot and N&E Associates, were participating in a check-pooling scheme whereby: (1) the afore-mentioned outlets transferred the proceeds of fraudulent received transactions to another MoneyGram outlet, "Modicom Accounting"; and (2) Modicom Accounting then deposited the fraud proceeds into a single bank account in its name. In response, one member of the Fraud Department wrote the following to other Fraud Department personnel, including the then Director of AML Compliance and Fraud: "Modicom is a suspect agent location that we're aware of . . . ."

74. None of the above-referenced outlets — Money Spot, N&E Associates or Modicom Accounting — was terminated during Haider's tenure at MoneyGram; all were terminated within one year of his departure.

75. In addressing MoneyGram's failure to terminate outlets that the Fraud Department had recommended for termination in early 2007, Haider has since acknowledged that "[t]hey don't seem to be [close calls on whether to terminate]." He further stated: "I'm thinking I must have dropped the ball somewhere. . . . I mean business might have asked for more data, as I said, but at some point we should have gone forward and terminated them."

When asked specifically, "[w]hose fault is [it] . . . [t]hat Money Spot was not closed, who's fault?" Haider responded, "I told you the buck stops with me."

d) Subsequent to April 2007, Outlets Identified on the April 2007 Spreadsheets Continued to Engage in Fraud

76. After April 2007, MoneyGram continued to receive complaints from its customers indicating that outlets that had been identified on the April 2007 Spreadsheets were continuing to engage in fraudulent schemes. For example, from May 2007 through May 2008 (when Haider left MoneyGram): (1) Money Spot accumulated approximately 345 Consumer Fraud Reports, totaling more than $600,000 in consumer losses; (2) Money Spot 2 accumulated approximately 67 Consumer Fraud Reports, totaling more than $80,000 in consumer losses; (3) Money Spot 5 accumulated approximately 36 Consumer Fraud Reports, totaling more than $26,000 in consumer losses; and (4) N&E Associates accumulated approximately 40 Consumer Fraud Reports, totaling more than $90,000 in consumer losses.

c. Haider Allowed the Sales Department to Influence the Agent/Outlet Discipline Process

77. In addition to failing to implement a discipline policy and failing to terminate known high-risk agents, Haider allowed the agent/outlet review process to function such that when the Fraud Department wanted to terminate an agent/outlet, it generally had to consult with the Sales Department before doing so. In an email dated June 25, 2007, a MoneyGram employee with responsibilities related to AML compliance and fraud (who had previously been the Director of AML Compliance and Fraud) informed MoneyGram's then Director of Fraud (who had recently been hired) that before closing an agent, "[w]e need to go to management and sales to make the case to close." This consultation process resulted in instances where efforts by the

Fraud Department to terminate or otherwise discipline known high-risk agents were frustrated or delayed.

78. Haider had the authority to terminate agents/outlets. Therefore, to the extent the Sales Department or others successfully resisted any such terminations — including in connection with the April 2007 Spreadsheets — Haider allowed it to happen.

2. Haider Failed to Implement Policies to Ensure that MoneyGram Complied with Its Obligation to File Timely SARs

79. Although Haider was well aware of the nature and extent of the consumer fraud information collected and maintained by the Fraud Department, he maintained MoneyGram's AML program such that the analysts responsible for filing SARs ("SAR analysts") were not provided with information from the Fraud Department's Consumer Fraud Report database, including information identifying specific outlets that had accumulated excessive numbers of Consumer Fraud Reports. Moreover, Haider did not otherwise ensure that the Fraud Department shared relevant information with the SAR analysts, or provide adequate direction to staff on when SARs should be filed relating to fraud. As a result, the Fraud Department failed to refer incidents of known or suspected consumer fraud or money laundering to the SAR analysts. Consequently, those analysts lacked the information they needed to file the required SARs. This arrangement — maintaining separate "silos" of information within MoneyGram's various departments such that MoneyGram's SAR analysts did not possess relevant information — was in place throughout Haider's employment at MoneyGram.

80. Haider's failure to ensure that the Fraud Department provided relevant information to MoneyGram's SAR analysts was contrary to guidance he received from one of MoneyGram's external AML compliance consultants in 2005. The consultant advised Haider as follows:

> Recently, financial institutions have been criticized for not including within their SAR monitoring procedures activity occurring at different business lines or locations. For example, a bank was recently the subject of criminal and civil sanctions, in part, because of its failure to file SARs on fraudulent activity that was the subject of substantial litigation within the bank. In this instance, its litigation department was defending the bank against claims by numerous investors who had been victimized by in [sic] an illegal investment scheme run by customers of the bank. Unfortunately, the department did not inform its AML office and no SARs were filed. The failure of the bank to file SARs in this instance led, in part, to the criminal charges against the bank and a $40 million criminal forfeiture.
>
> In another recent case, a bank faced substantial criminal and civil sanctions for failing to file SARs on customers who were named in grand jury subpoenas received by the bank. While the AML regulatory requirements that apply to banks are different from those for MSBs, it is important that [MoneyGram's] AML compliance office receive information about suspected criminal activity no matter where in the organization that activity may have been discovered. Similarly, it is recommended that when MoneyGram receives federal or state grand jury subpoenas it should consider notifying the AML office (or some other centralized office) so that a determination can be made whether to investigate the matter further and, in appropriate cases, to file a SAR if the subject of the subpoena had utilized [MoneyGram's] financial products.

81. In late 2007, a different AML consultant recommended that Haider consider developing a formal policy and providing further guidance to staff with respect to the situations in which SARs should be filed that are related to fraud.

82. Haider's failure to ensure that MoneyGram's SAR analysts received all relevant information, and that MoneyGram's fraud and AML personnel were properly trained on the filing of SARs relating to fraud, caused SARs against known high-risk agents/outlets to be filed significantly late or not at all. In some cases, SARs against known high-risk agents/outlets were filed well over a year after MoneyGram personnel had identified suspicious conduct.

83. Additionally, and compounding the consumer harm, many of the SARs that MoneyGram did file incorrectly listed the victim of the fraud as the subject (*i.e.*, the suspected wrongdoer) and/or identified the known or suspected complicit agent merely as the transaction location (*i.e.*, the physical location where the suspicious activity had occurred).

84. Part I *infra* (paragraphs 96 to 108) includes specific examples of instances where MoneyGram failed to fulfill its obligation to file timely SARs, including failures that occurred during the Assessment Period.

3. Haider Failed to Ensure that MoneyGram Performed Proper Audits of Its Agents and Outlets

85. Haider also failed to ensure that MoneyGram complied with the BSA requirement to conduct adequate risk-based audits of its agents/outlets.

86. As an initial matter, MoneyGram did not consistently perform risk-based audits of agents/outlets, even those that it had identified as (1) having accumulated an excessive number of Consumer Fraud Reports, and/or (2) possessing other high-risk characteristics. For example, as of December 2005, MoneyGram had not done any compliance audits in Canada. Yet, prior to that date, the Fraud Department suspected that numerous agents/outlets in Canada were participating in fraud. One such outlet was recommended by the Fraud Department for "closure/restriction" as early as January 2005. A January 2005 document recommending the "closure/restriction" of that outlet indicted that the outlet had opened in February 2003 and, as of January 2005, had: (1) "56 reported complaints of consumer fraud . . . totaling $104,166"; and (2) processed 950 receive transactions, 869 of which were sent from the United States. This same outlet was later identified on spreadsheets that were sent to Haider on or about March 15, 2007, as having received 44 fraud-induced money transfers in 2005 and 26 fraud-induced money transfers in 2006, which constituted 17.9% and 9.4% of the outlet's total number of received money transfers for those years, respectively. Moreover, the outlet had the vast majority of its received money transfers originate in the United States, and an average dollar value of received money transfers that exceeded $1,000. Notwithstanding these clear signs of fraud, this outlet

remained open throughout Haider's employment at the Company; it was eventually terminated in March 2009.

87. Even after December 2005, MoneyGram did not perform risk-based audits of known high-risk agents/outlets in Canada. For example, Money Spot was not audited during Haider's employment at MoneyGram.

88. Moreover, to the extent MoneyGram performed audits of agents/outlets, they were frequently ineffective. With respect to on-site audits, for example, MoneyGram's former Senior Director of AML Compliance has confirmed that on-site auditors were not trained to look for warning signs of fraud. Nor did on-site auditors otherwise conduct adequate AML reviews. For example, they did not review copies of the MoneyGram transfer checks that the outlets had issued in paying out received money transfers, to see if the checks had been made payable to another MoneyGram outlet. (When one MoneyGram outlet makes a MoneyGram transfer check payable to another MoneyGram outlet, that is an indication that the outlets are participating in a check-pooling scheme.) This failure to review transfer checks was significant given that no later than January 2007, MoneyGram's then Director of AML Compliance and Fraud, as well as other members of MoneyGram's Fraud Department, possessed evidence demonstrating that various MoneyGram outlets were participating in a check-pooling scheme, as discussed above.

89. An email chain dated July 27, 2007, further demonstrates that, during Haider's tenure at MoneyGram, the Company's oversight of its agents/outlets was flawed and ineffective. In that email chain, a member of MoneyGram's Risk Department described his recent visits to multiple agents/outlets in Canada that were known or suspected to be participating in fraud and/or money laundering schemes to two members of MoneyGram's Fraud Department. These visits — which were informal and did not constitute "audits" — were similarly ineffective:

- Describing his visit to one particular outlet (which was one of the outlets identified on the April 2007 Spreadsheets), the Risk Department employee stated that he "didn't feel confident [sic] taking a picture of the place because [the agent's brother] looks like an enforcer (big guy that says little)." The Risk Department employee further stated that when the agent complained about the outlet's daily transaction limit, he (the Risk Department employee) "didn't feel it was the place to say to stop committing fraud and your limit won't be a problem." The Risk Department employee also noted that the agent was "a former . . . agent [of another money transmission company]," which the Risk Department employee stated "didn't surprise [him]." Subsequently, one of the Fraud Department employees wrote to the other: "Says a lot that he didn't feel comfortable taking a picture." This outlet remained open throughout Haider's employment at MoneyGram; it was terminated in March 2009.

- In the same July 27, 2007, email exchange, the MoneyGram Risk Department employee also described his interactions with another agent whose outlet had accumulated more than 130 Consumer Fraud Reports during the prior year (and was also identified on the April 2007 Spreadsheets): "Several weeks before my visit[] I spoke with [the agent] about the receive transactions and NSFs [transactions with insufficient funds]. At that time I warned him about the fraud and advised him we are watching all transactions. He got a good laugh and seemed to be very happy to see me." The Risk Department employee observed that this agent was also a former agent of another money transmission company. Notably, in January 2007, one of the Fraud Department employees on this email exchange had identified this agent's outlet as one of the outlets involved in the check-pooling scheme described in paragraph 75 above. This outlet remained open throughout Haider's employment at MoneyGram; it too was terminated in March 2009.

- In the same email exchange, the Risk Department employee stated that he had met James Ugoh, the owner/operator of the Money Spot outlets and N&E Associates: "I met Chief James Ugoh. I liked him, seems to be a genuine person. He is also very interest [sic], he is the younger chief and has been appointed the next elder chief of his tribe. . . . James also works at [a car rental company] (2nd shift) in [its] maintenance department. I found this very odd for a Chief and owner of 10 stores." Subsequently, one of the Fraud Department employees emailed the other: "Geez . . . ridiculous. Especially when he says 'I met Chief James Ugoh. I liked him, seems to be a genuine person.' Of course he's gonna act genuine even though his stores have probably paid over 200 fraud combined." All of Ugoh's outlets remained open throughout Haider's employment at MoneyGram, and all were terminated thereafter.

90. Notably, some MoneyGram agents/outlets that Haider failed to terminate were not subjected to audits precisely because the agents/outlets were understood to be engaging in fraud. In connection with the initial list of approximately 30 outlets that the Fraud Department had recommended for termination in early 2007, MoneyGram's former Senior Director of AML

Compliance did not have her staff conduct audits of those outlets because she was already "working with the assumption that the[y] were criminal operations," and sending MoneyGram's audit team into those outlets would put them in "physical danger." The former Senior Director of AML Compliance "strongly" expressed this view to Haider in 2007. As set forth above, the majority of those outlets were not terminated by Haider, including Money Spot, which the former Senior Director of AML Compliance has characterized as "the worst of even the group of agents that we were concerned about."

91. Moreover, throughout Haider's employment at MoneyGram, MoneyGram's process of identifying agents/outlets to audit was fundamentally flawed and ineffective due to a lack of information sharing between the Fraud and AML Compliance Departments. When the AML Compliance Department decided which agents/outlets to audit, it did not consider the number of Consumer Fraud Reports that MoneyGram's agents/outlets had accumulated. MoneyGram's former Senior Director of AML Compliance has since acknowledged that agents with highly elevated levels of fraud presented a higher risk of money laundering.

4. Haider Failed to Ensure that MoneyGram Adequately Screened New Agents and Outlets

92. Throughout his employment at MoneyGram, Haider also failed to ensure that MoneyGram conducted adequate due diligence on prospective MoneyGram agents. Similarly, Haider failed to ensure that MoneyGram conducted adequate due diligence on existing MoneyGram agents seeking to open additional MoneyGram outlets.

93. Under Haider, MoneyGram personnel allowed new agents to open outlets, and existing agents to open additional outlets, without taking steps to verify that a legitimate business did or could exist at the proposed outlet sites. As a result, MoneyGram agents were permitted to operate outlets out of homes in residential neighborhoods and other locations that were not open

to the public. Agents operating out of such locations were clearly not offering legitimate money transmission services. For example, Money Spot 9 operated out of a house in a residential neighborhood. Similarly, due to the lack of an adequate review process, Ugoh was allowed to open Money Spot 7 in a location only a few feet away from Money Spot 5. Money Spot 5 was located at 1708 Weston Road in Toronto, while Money Spot 7 was located at 1714 Weston Road in Toronto.

94. Additionally, under Haider, MoneyGram allowed numerous agents to open MoneyGram outlets despite the fact that the agents had previously been terminated by another money transmission company. In evaluating new agents, MoneyGram did not inquire whether they had previously been terminated by another money transmission company, notwithstanding that MoneyGram personnel recognized that prior terminations were an indicator of fraud. In an email dated February 2, 2005, MoneyGram's then Director of AML Compliance and Fraud observed that when an agent sought to become affiliated with MoneyGram after being affiliated with another money transmission company, it was likely that the agent had been terminated by the other money transmission company "due to fraud concerns." Moreover, as set forth in paragraph 90 above, personnel within MoneyGram's Fraud and Risk Departments knew or suspected that agents that had come to MoneyGram from another money transmission company were engaging in fraud while at MoneyGram.

95. The lack of coordination between MoneyGram's various departments also resulted in MoneyGram granting additional outlets to agents known or suspected to be involved in fraud and/or money laundering. For example, by the time of Haider's separation from MoneyGram in May 2008, MoneyGram had allowed Ugoh to expand his network to 12 outlets. As of March 2008, Fraud Department personnel understood that multiple of those outlets were

participating in fraud and/or money laundering schemes. Nevertheless, during that month, Ugoh was authorized to open the last of his outlets, Money Spot 11, even though his other outlets had by then accumulated more than 750 Consumer Fraud Reports, totaling well over $1 million in consumer losses.

I. Haider Willfully Failed to Ensure that MoneyGram Filed Timely Suspicious Activity Reports

96. As set forth in Part H. above, under Haider, MoneyGram's AML program was fundamentally flawed because the Fraud Department did not share important information with the analysts responsible for filing SARs. Among other things, information from the Consumer Fraud Report database was not provided to those SAR analysts. Nor did the Fraud Department have a consistent practice of communicating its concerns about particular agents or outlets to the SAR analysts. Haider also failed to provide adequate direction to staff regarding the filing of SARs relating to fraud. As a result, there were numerous agents/outlets that had accumulated an extraordinary number of Consumer Fraud Reports and/or that members of the Fraud Department had identified as likely participating in fraud and/or money laundering, but for which MoneyGram: (1) did not file any SARs; (2) filed SARs, but exceedingly late; or (3) filed SARs, but improperly identified the suspect agents/outlets merely as the transaction locations (*i.e.*, the physical locations where the suspicious activity had taken place), rather than the subjects of the SARs (*i.e.*, the suspected wrongdoers).

1. Examples of SAR Violations Involving Agents/Outlets that Had Accumulated Excessive Numbers of Consumer Fraud Reports and Other Red Flags

96. A January 30, 2007, email from MoneyGram's then Director of AML Compliance and Fraud to, among others, its then Senior Director of AML Compliance illustrates the Company's deficient SAR-filing practices under Haider. The Director explained that a

particular outlet in Houston, Texas, had been closed in 2006 after "Fraud . . . review[ed its] activity and found 46 reported consumer fraud payouts at th[e] location," which "was 9% of total receives and unacceptable." The Director said that she "plan[ned] to say only that to the examiners." The Director then went on to state:

> This activity was after we stopped directed sends to Canada. It appear[s] that the owners or others at [this outlet] were working with individuals in Canada. Once the funds could not be paid in Canada, the fraud perps found locations in the USA and directed those locations to receive the funds and send the money to CD [Canada] after taking a cut. **I don't want to go into this level because I'm not sure if SARs were filed on the agent at the time — we should have. We closed several locations in TX and several in NY that all had the same pattern of involvement in CD [Canadian] lottery fraud.**

(Emphasis in original). In other words, MoneyGram's Director of AML Compliance and Fraud had identified this outlet as having likely participated in a fraudulent scheme. MoneyGram personnel referred to this type of scheme as "flipping," where a fraudulent outlet in the United States received a fraud-induced money transfer and then immediately sent (or flipped) the money to another fraudulent outlet in Canada. Additionally, in March 2007, MoneyGram received a law enforcement subpoena directed at this outlet. However, MoneyGram did not file a SAR on this outlet or its agent/owner at the time it closed the outlet, at the time it received the subpoena, or at any other time during Haider's employment at MoneyGram.

97. Similarly, in March 2007, a Fraud Department analyst identified Abbey One Stop, a MoneyGram outlet in Orange, New Jersey, as a potential participant in the same type of flipping scheme referenced in the prior paragraph. In August 2007, another MoneyGram employee sent the then Director of Fraud an email identifying five "Bad Agents" that "receive consumer fraud," one of which was "Abbey One Stop" (the outlets discussed below in paragraphs 99 and 100 were also identified in this email). A few months later, in January 2008 and February 2008, MoneyGram received two law enforcement subpoenas directed at Abbey

One Stop. Shortly thereafter, on April 4, 2008, multiple Fraud Department employees, including the Director of Fraud, received an email from another MoneyGram employee suggesting that Abbey One Stop had improperly removed funds from MoneyGram's money transfer system. The email further noted, "[w]e have received several complaints about . . . Abbey One Stop . . . . Other cases involve consumer fraud and it is received at this particular agent." From October 2006 through April 23, 2008 (*i.e.*, approximately 30 days before the end of the Assessment Period), Abbey One Stop accumulated approximately 156 Consumer Fraud Reports, totaling more than $395,000 in consumer losses. Moreover, during the period from November 15, 2007 (*i.e.*, the beginning of the Assessment Period), through April 23, 2008, Abbey One Stop accumulated approximately 28 Consumer Fraud Reports, totaling more than $70,000 in consumer losses. And, during the six months immediately preceding the Assessment Period, Abbey One Stop accumulated approximately 75 Consumer Fraud Reports, totaling more than $190,000 in consumer losses. Nevertheless, MoneyGram did not file a SAR identifying Abbey One Stop or its agent/owner, Festus Abbey ("Abbey"), as the subject until April 2009.[8] Abbey ultimately pled guilty to one count of conspiracy to commit mail and wire fraud in connection with consumer fraud schemes, and was sentenced to 41 months' imprisonment. Abbey One Stop remained a MoneyGram outlet throughout Haider's employment at the Company; it was terminated in August 2009.

98. As another example of MoneyGram's deficient SAR-filing practices under Haider, in February 2006, a Fraud Department analyst identified an outlet in San Ysidro,

[8] When this Assessment refers to an outlet or its agent/owner not being identified as the "subject" of a SAR, it means that neither the outlet nor its agent/owner was identified as a potential wrongdoer in a SAR; at most, the outlet was identified in one or more SARs merely as the physical location from which one or more of the money transfers at issue in the SAR(s) had been sent or received.

California, as having a high number of fraud payouts and recommended that action be taken against the outlet. Thereafter, in August 2007, the then Director of Fraud identified the same outlet as having accumulated more than 200 Consumer Fraud Reports during the seven-month period from January 2007 through July 2007, totaling approximately $300,000 in consumer losses. In August 2007, the Director of Fraud recommended that this outlet be terminated immediately, characterizing it as one of the "worst of the worst." However, the outlet was not terminated, and from November 15, 2007, through April 23, 2008, it accumulated approximately 130 more Consumer Fraud Reports, totaling nearly $200,000 in consumer losses. During Haider's employment at MoneyGram, the Company did not file any SARs identifying this outlet or its agent/owner as the subject; it first filed such a SAR in April 2009. The outlet remained a MoneyGram outlet throughout Haider's employment at the Company; it was terminated in June 2009.

99. In August 2007, the Director of Fraud also identified another outlet — this one located in Brooklyn, New York — as a high fraud outlet. At that time, the Director of Fraud observed that this outlet had accumulated 41 Consumer Fraud Reports since January 2007, totaling approximately $65,000 in consumer losses. Thereafter, the outlet continued to accumulate a significant number of Consumer Fraud Reports. From November 15, 2007, through April 23, 2008, it accumulated approximately 18 Consumer Fraud Reports, totaling more than $55,000 in further consumer losses. And, during the six months preceding the Assessment Period, the outlet accumulated approximately 30 Consumer Fraud Reports, totaling more than $70,000 in consumer losses. In late 2007 or early 2008, the Director of Fraud identified this outlet as one of the top three fraud outlets in New York. Yet, during Haider's employment at MoneyGram, the Company did not file any SARs identifying this outlet or its

agent/owner as the subject; it first filed such a SAR in April 2009. The outlet remained open throughout Haider's employment at the Company; it was terminated in May 2009.

100. In late 2007 or early 2008, the Director of Fraud identified yet another outlet — this one located in Houston, Texas — as a high fraud outlet, and one of the top two fraud outlets in Texas. At that time, the Director of Fraud noted that the outlet had accumulated 95 Consumer Fraud Reports in 2007, totaling more than $230,000 in consumer losses. Moreover, from November 15, 2007, through April 23, 2008, this outlet accumulated approximately 80 Consumer Fraud Reports, totaling more than $210,000 in consumer losses. And during the six months immediately preceding the Assessment Period, the outlet accumulated approximately 51 Consumer Fraud Reports, totaling more than $130,000 in consumer losses. In March 2007, MoneyGram received a law enforcement subpoena directed at this outlet. Despite all of the above, MoneyGram did not file a SAR identifying this outlet or its agent/owner as the subject during Haider's employment at the Company; it first filed such a SAR in April 2009. The outlet remained a MoneyGram outlet throughout Haider's employment at the Company; it was terminated in May 2009.

101. Below are additional examples of MoneyGram outlets that, during Haider's employment at the Company, accumulated an excessive number of Consumer Fraud Reports and yet were not identified as the subject of any timely-filed SARs:

- Miracle Multi-Link, a MoneyGram outlet in Brooklyn, New York, accumulated more than 340 Consumer Fraud Reports, totaling over $1.2 million in consumer losses, from 2007 through 2009. The owner of this outlet, Itohan Agho Allen, was ultimately convicted of conspiracy to commit mail fraud, wire fraud, and money laundering, and sentenced to 180 months' imprisonment. During Haider's employment at MoneyGram, the Company did not file any SARs identifying this agent/outlet as the subject, notwithstanding that: (1) in late 2007 or early 2008, the Director of Fraud received a spreadsheet identifying this outlet as among the top five fraud outlets in New York (he noted that in 2007, the outlet had received 17 Consumer Fraud Reports, totaling more than $47,000 in consumer losses); and (2) from November 15, 2007, through April

23, 2008, the outlet accumulated approximately 55 Consumer Fraud Reports, totaling more than $180,000 in consumer losses. Miracle Multi-Link remained a MoneyGram outlet throughout Haider's employment at the Company; it was terminated in May 2009.

- An additional MoneyGram outlet located in Austell, Georgia accumulated more than 360 Consumer Fraud Reports, totaling over $1 million in consumer losses, from 2007 through 2008. During Haider's employment at MoneyGram, the Company did not file any SARs identifying this outlet or its agent/owner as the subject, notwithstanding that, from November 15, 2007, through April 23, 2008, the outlet accumulated approximately 30 Consumer Fraud Reports, totaling more than $75,000 in consumer losses. And during the six months immediately preceding the Assessment Period, the outlet accumulated approximately 33 more Consumer Fraud Reports, totaling more than $95,000 in additional consumer losses. This outlet remained open throughout Haider's employment at MoneyGram; it was terminated in January 2009.

- Another MoneyGram outlet located in Houston, Texas, accumulated more than 160 Consumer Fraud Reports, totaling over $530,000 in consumer losses, from 2007 through 2008. During Haider's employment at MoneyGram, the Company did not file any SARs identifying this outlet or its agent/owner as the subject, notwithstanding that, from November 15, 2007, through April 23, 2008, the outlet accumulated approximately 48 Consumer Fraud Reports, totaling more than $135,000 in consumer losses. This outlet remained open throughout Haider's employment at MoneyGram; it was terminated in January 2009.

- During the period from November 15, 2007, through April 23, 2008, the additional outlets referenced in the chart below also accumulated an excessive number of Consumer Fraud Reports. However, during Haider's employment at MoneyGram, the Company did not file any SARs in which any of the below outlets or their agent/owners were identified as the subject. Notably, in November 2007, MoneyGram received a law enforcement subpoena targeting one of the below outlets (the one with 89 Consumer Fraud Reports). Moreover, in late 2007 or early 2008, the Director of Fraud received a spreadsheet identifying this outlet as among the top five fraud outlets in Texas (he noted that in 2007, the outlet had received 39 Consumer Fraud Reports, totaling more than $135,000 in consumer losses). In an email dated April 3, 2008, a MoneyGram employee with responsibilities relating to AML compliance and fraud (who had previously been the Director of AML Compliance and Fraud) wrote the following to, among others, the then Director of Fraud about that outlet: "Are you looking into [the outlet] and [its] potential involvement in consumer fraud? I attempted to confirm rcvr info on 3-4 transactions and nothing checked out . . . . My concern is that this is another agent in [Texas] who is working with the Nigerians in Canada on consumer frauds . . . ."

Outlet Location	Approximate Number of Consumer Fraud Reports Accumulated From 11/15/07 Through 4/23/08	Losses Associated with Consumer Fraud Reports Referenced in Prior Column	Date Terminated by MoneyGram
Austell, Georgia	70	$106,957.04	3/11/09
Rialto, California	49	$147,677.02	11/10/08
Newark, New Jersey	53	$169,186.17	6/1/09
Houston, Texas	89	$300,074.59	12/31/08
Houston, Texas	87	$259,569.16	11/13/08
Brooklyn, New York	37	$129,273.93	11/7/08

2. Examples of SAR Violations Involving Agents/Outlets that Had Been Recommended to Haider for Termination

102. Under Haider, MoneyGram also failed to file timely SARs on a number of the specific outlets that were proposed to him and others for termination in April 2007. Nor were SARs filed on those outlets' agent/owners. As discussed above, Ugoh owned and/or operated four of those outlets: Money Spot, Money Spot 2, Money Spot 5, and N&E Associates. Although Ugoh operated these and his nine other outlets in Canada, the outlets received more than $27.8 million in money transfers from the United States. Ugoh has admitted that almost all of the money his outlets received from the United States constituted fraud proceeds.

103. Haider was on notice of Ugoh's fraudulent activities as early as 2004, and of those activities' connection to U.S. consumers no later than April 2007, when he was sent the above-referenced April 2007 Spreadsheets. *See supra* paragraphs 63 to 70. Those spreadsheets included the following information for Money Spot, Money Spot 2, Money Spot 5, and N&E Associates, relating to the six-month period from September 2006 through February 2007:

Outlet Name	# of Received Trans-actions Reported as Fraudulent	% of Received Trans-actions Reported as Fraudulent	$ Amount of Fraud-Induced Trans-actions	# of Received Trans-actions	# of Received Trans-actions from the U.S.	% of Received Trans-actions from the U.S.
Money Spot	36	5.80%	$84,067.37	621	517	83.25%
Money Spot 2	21	7.34%	$40,699.07	286	259	90.56%
Money Spot 5	58	9.34%	$99,489.26	621	560	90.18%
N&E Associates	35	10.29%	$79,730.70	340	321	94.41%

The April 2007 Spreadsheets also revealed that Money Spot, Money Spot 2, Money Spot 5, and N&E Associates had high percentages of their total number of received money transfers reported as fraudulent in prior years as well:

Outlet Name	% of Received Transactions Reported as Fraudulent in 2006	% of Received Transactions Reported as Fraudulent in 2005	% of Received Transactions Reported as Fraudulent in 2004
Money Spot	8.7%	7.8%	4.49%
Money Spot 2	8.27%	7.04%	1.3%
Money Spot 5	10.42%	Not open yet	Not open yet
N&E Associates	11.22%	13.58%	7.41%

Additionally, the April 2007 Spreadsheets indicated that MoneyGram had received law enforcement subpoenas directed at Money Spot, Money Spot 2, Money Spot 5, and N&E Associates. In fact, MoneyGram had received law enforcement subpoenas directed at those outlets in June 2005 (Money Spot), August 2005 (Money Spot), March 2006 (Money Spot, Money Spot 2 and N&E Associates), May 2006 (Money Spot, Money Spot 2 and N&E Associates), and February 2007 (Money Spot, Money Spot 2 and Money Spot 5). During

Haider's employment at MoneyGram, the Company also received law enforcement subpoenas directed at Money Spot 4 (February 2007) and Money Spot 6 (March 2007).

104. Nevertheless, during Haider's employment at MoneyGram, the Company never filed a SAR identifying Ugoh or any of his outlets as the subject. Instead, during that time, MoneyGram facilitated Ugoh's fraudulent activities in a number of ways — and turned a blind eye to his misconduct — as detailed in the following chronology:

- In August 2004, MoneyGram's then Director of AML Compliance and Fraud recognized that Ugoh's initial MoneyGram outlet, Money Spot, had an unusually high number of fraud complaints. In August 2004, the Director of AML Compliance and Fraud also learned, and informed Haider, that the Toronto Police Department regarded Money Spot as "dirty." Nevertheless, that same month, MoneyGram authorized Ugoh to open two additional outlets, Money Spot 2 and Money Spot 3.

- In March 2005, MoneyGram authorized Ugoh to open another outlet, Money Spot 4.

- In November 2005, a Fraud Department analyst identified a number of Canadian outlets that he characterized as "bad," all of which had received between 39 and 127 fraud-induced money transfers in 2005. The analyst recognized that Money Spot had accumulated 46 Consumer Fraud Reports in 2005 and 136 Consumer Fraud Reports in total, and that the 136 Consumer Fraud Reports had resulted in $489,238 in consumer losses.

- In February 2006, MoneyGram's Fraud Department identified Money Spot, Money Spot 2, and N&E Associates as leading fraud outlets.

- In June 2006, MoneyGram authorized Ugoh to open a fifth outlet, Money Spot 5.

- In July 2006, MoneyGram's Risk Department contemplated permanently restricting Money Spot's ability to receive transactions because of fraud, but the restriction was not implemented.

- In August 2006, MoneyGram authorized the opening of Money Spot 6, and the following month, paid Ugoh a $70,000 "re-signing bonus."

- As of January 2007, MoneyGram's then Director of AML Compliance and Fraud and other Fraud Department personnel were on notice that Money Spot was working with other MoneyGram agents in connection with the above-described check-pooling scheme.

- In March 2007, MoneyGram authorized Ugoh to open Money Spot 7 and Money Spot 8, notwithstanding that his other outlets had by then accumulated hundreds of Consumer Fraud Reports. During the month of March 2007 alone, Ugoh's outlets accumulated approximately 35 Consumer Fraud Reports, totaling more than $60,000 in consumer losses.

- In April 2007, MoneyGram's Fraud Department recommended the termination of Money Spot, Money Spot 2, Money Spot 5, and N&E Associates as part of its above-referenced effort to terminate MoneyGram's worst high-fraud Canadian outlets. Despite this recommendation, MoneyGram allowed all of Ugoh's outlets to remain open; none of those outlets was closed while Haider was employed at MoneyGram.

- In June 2007, MoneyGram authorized Ugoh to open Money Spot 9 and Money Spot 10.

- In July 2007, MoneyGram awarded Money Spot the status of "Red Store," MoneyGram's corporate marketing award for its top-performing outlets. Also in July 2007, MoneyGram's internal Fraud Report listed Money Spot as one of the Company's top fraud outlets.

- In August 2007, MoneyGram increased Ugoh's commission, and made the commission increase retroactive to September 2006.

- In December 2007, Money Spot again was listed as a top fraud outlet on MoneyGram's internal Fraud Report. Money Spot, Money Spot 2, Money Spot 4, and N&E Associates were all in the top nine for fraud in Ontario. And, in late 2007 or early 2008, MoneyGram's then Director of Fraud identified those four outlets as having received 298 fraud-induced money transfers in 2007, totaling more than $600,000 in consumer losses.

- In February 2008, a MoneyGram employee with responsibilities relating to AML compliance and fraud (who had previously been the Director of AML Compliance and Fraud) identified new potentially fraudulent behavior involving Money Spot, prompting a Fraud Department analyst to write the following in an email to the afore-mentioned employee and the then Director of Fraud: "[Y]ou recall James [Ugoh]. He's the Nigerian Chief that was 'very concerned' with the fraud that ran through his store when we suggested agent closure last year or the year before. He was so concerned, he convinced Sales and Risk he'd call . . . Risk when he felt a fraudster was attempting to receive a transaction. However, what he was doing is calling us on the $800-$1100 transactions and still paying out the higher dollar amounts. I think those phone calls last[ed] about 3 months. This particular store is currently our highest receive location in Toronto."

- In March 2008, MoneyGram authorized Ugoh to open Money Spot 11, notwithstanding that Ugoh's other outlets had by then accumulated more than 750 Consumer Fraud Reports.

- From November 15, 2007, through April 23, 2008, Ugoh's outlets accumulated more than 380 Consumer Fraud Reports, totaling more than $600,000 in consumer losses. Moreover, during the above-referenced period, Money Spot itself accumulated more than 175 Consumer Fraud Reports, totaling more than $280,000 in consumer losses.

105. Notwithstanding the information set forth in the above chronology — including that Ugoh's outlets had accumulated more than 380 Consumer Fraud Reports from November 15, 2007, through April 23, 2008 — during Haider's employment at MoneyGram, the Company never filed a SAR identifying Ugoh or any of his outlets as the subject.

106. In September 2008, MoneyGram closed Money Spot 6, and it closed Ugoh's remaining outlets in February 2009. In October 2009, Ugoh was charged with various crimes relating to consumer fraud, and he pled guilty to one count of conspiracy to commit wire fraud and money laundering, as well as one count of mail fraud. Ugoh was subsequently sentenced to 151 months' imprisonment.

107. In addition to Money Spot, Money Spot 2, Money Spot 5, and N&E Associates, many of the other outlets that were proposed for closure in April 2007 also had (1) tens of thousands of dollars in fraud-induced transactions and (2) significant contacts with the United States. Two of those outlets are listed below. All of the information that appears below in connection with the two outlets appeared on the April 2007 Spreadsheets.

- Outlet 1. This outlet — which had 26 of its 394 receive transactions (6.6%) reported as fraudulent during the six-month period from September 2006 through February 2007 — had 381 of those 394 receive transactions (96.7%) originate from the United States. The 26 fraudulent receive transactions totaled more than $70,000 in consumer losses.

- Outlet 2. This outlet — which had 61 of its 702 receive transactions (8.6%) reported as fraudulent during the above-referenced six-month period — had 626

> of those 702 receive transactions (89.1%) originate from the United States. The 61 fraudulent receive transactions totaled more than $80,000 in consumer losses.

Moreover, at least some of those other outlets that were proposed for termination in April 2007 — including Outlet 1 and Outlet 2 — continued to accumulate significant numbers of Consumer Fraud Reports thereafter. For example, from November 15, 2007, through April 23, 2008, Outlet 1 and Outlet 2 accumulated approximately 25 and 37 Consumer Fraud Reports, respectively. During Haider's employment at MoneyGram, the Company also received law enforcement subpoenas directed at Outlet 1 (in February 2008) and Outlet 2 (in March 2007). Moreover, in an email dated April 30, 2008, a Fraud Department analyst observed that Outlet 1 was likely participating in a flipping scheme with another outlet located in New York. Nevertheless, during Haider's employment at MoneyGram, neither Outlet 1 nor Outlet 2 (or their agents/owners) was the subject of a SAR, and neither was terminated. Outlet 1 was ultimately terminated in December 2008, and Outlet 2 was terminated in June 2009.

108. As a result of MoneyGram's failure to file timely SARs under Haider, the perpetrators of fraudulent schemes were allowed to continue to defraud the public without the requisite notice being provided to FinCEN. Through FinCEN, law enforcement agencies may access SARs and use them to: (1) initiate criminal and civil investigations; (2) expand existing investigations and uncover previously unidentified co-conspirators and undetected money trails; (3) facilitate information exchange with law enforcement counterparts worldwide; and (4) identify relationships between illicit actors and their financing networks, thereby allowing the disruption of such networks and the prosecution of their participants. Haider's failure to ensure that MoneyGram filed proper and timely SARs deprived law enforcement of critical information it could have used for these purposes.

III. CONCLUSION AND ASSESSMENT

MoneyGram was required to implement and maintain an effective AML program, as set forth in the BSA and its implementing regulations. As MoneyGram's Chief Compliance Officer, Haider was responsible for ensuring that MoneyGram implemented and maintained an effective AML program. As set forth above, throughout his employment at MoneyGram — including during the Assessment Period — Haider failed to ensure that MoneyGram implemented and maintained an effective AML program. Among other things, Haider failed to: (1) implement a policy for disciplining high-risk agents/outlets; (2) ensure that unambiguously high-risk agents/outlets of which he was on notice were terminated; (3) ensure that there was sufficient coordination between MoneyGram's Fraud Department and MoneyGram's SAR analysts, such that timely SARs were filed on agents/outlets that the Fraud Department had identified as, among other things, having accumulated an excessive number of Consumer Fraud Reports; (4) ensure that high-risk agents/outlets were subjected to proper audits; or (5) ensure that MoneyGram adequately screened new agents, or existing agents seeking to open new outlets.

MoneyGram was required to file SARs on a timely basis, as set forth in the BSA and its implementing regulations. As MoneyGram's Chief Compliance Officer, Haider was responsible for ensuring that MoneyGram filed timely SARs when it knew, suspected, or had reason to suspect that specific agents and/or outlets were complicit in transactions that: (1) involved funds derived from illegal activity or were intended to hide or disguise funds derived from illegal activity; (2) were designed to evade the requirements of the BSA or its implementing regulations; (3) served no business or apparent lawful purpose; or (4) involved the use of MoneyGram's money transfer system to facilitate criminal activity.

As set forth above, Haider failed to ensure that MoneyGram's Fraud Department provided relevant information to the analysts responsible for filing SARs. Haider also failed to ensure that: (1) MoneyGram personnel received adequate guidance on the filing of SARs relating to fraud; or (2) MoneyGram filed timely SARs on agents and/or outlets that MoneyGram personnel knew or suspected were using MoneyGram's money transfer system to facilitate fraudulent activities. This resulted in MoneyGram failing to fulfill its SAR-reporting obligations in connection with specific agents/outlets throughout Haider's employment at MoneyGram, including during the Assessment Period.

FinCEN has determined that Haider willfully violated the BSA and its implementing regulations by failing to establish and implement an effective anti-money laundering program, and by failing to report suspicious activity as required by the BSA. FinCEN has further determined that grounds exist to assess a civil money penalty for these violations of the Act and its implementing regulations. FinCEN has determined that the penalty in this matter will be $1 million. 31 U.S.C. § 5321 and 31 C.F.R. § 1010.820.

FINANCIAL CRIMES ENFORCEMENT NETWORK

/S/ December 18, 2014

Jennifer Shasky Calvery Date
Director

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

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2014-07**
North Dade Community Development	)	
Federal Credit Union	)	
Miami Gardens, Florida	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network ("FinCEN") has determined that grounds exist to assess a civil money penalty against North Dade Community Development Federal Credit Union ("North Dade") pursuant to the Bank Secrecy Act ("BSA") and regulations issued pursuant to that Act.[1]

North Dade admits to the facts set forth below and that its conduct violated the BSA. North Dade consents to the assessment of a civil money penalty and enters the CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY ("CONSENT") with FinCEN.

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

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951–1959 and 31 U.S.C. §§ 5311–5314, 5316–5332. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Chapter X.

FinCEN has the authority to investigate credit unions for compliance with and violation of the Bank Secrecy Act pursuant to 31 C.F.R. § 1010.810, which grants FinCEN "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter." North Dade was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations during the time relevant to this action. 31 U.S.C. § 5312(a)(2)(E); 31 C.F.R. §§ 1010.100(d)(6), 1010.100(t)(1).

North Dade is a non-profit, federally chartered, community development financial institution located in Miami Gardens, Florida. The National Credit Union Administration ("NCUA") is North Dade's federal functional regulator and examines credit unions, including North Dade, for compliance with the BSA and its implementing regulations. North Dade was founded in 1997 to serve the North Dade/Broward County community area. Credit unions have authorized fields of membership, which means that a limited group of people and entities are eligible to be members of the credit union. North Dade's authorized field of membership is limited to individuals and entities that live, work, or worship in the North Dade County area. North Dade has one branch, with five employees, and assets of $4.1 million dollars.

North Dade's BSA failures derived significantly from its banking services to certain money services businesses ("MSBs"). These MSBs were located outside of its geographic field of membership and were engaged in high-risk activities, such as wiring millions of dollars per month to high-risk foreign jurisdictions. For instance, in 2013 alone, the total transaction volume through North Dade by MSBs included $54.8 million in cash orders, $1.01 billion in

outgoing wires, $5.3 million in returned checks, and $984.4 million in remote deposit capture.[2] North Dade's MSB activity accounted for 90% of North Dade's total annual revenue in 2013. This was not the expected business behavior of a small credit union like North Dade and led to substantial BSA compliance failures and violations.

II. DETERMINATIONS

FinCEN has conducted an investigation and determined that, from December 2009 through January 2014, North Dade willfully violated the BSA's program, reporting, and recordkeeping requirements.[3] NCUA cited North Dade for many of these violations in a Cease and Desist Order issued on September 6, 2013.

As described in more detail below, North Dade: (a) failed to implement an adequate anti-money laundering program, 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210; (b) failed to develop and implement an adequate customer identification program, 31 U.S.C. § 5318(l); 31 C.F.R. § 1020.220; (c) failed to detect and adequately report suspicious transactions, 31 U.S.C. § 5318(g); 31 CFR § 1020.320; and (d) failed to access or review FinCEN's 314(a) lists, 31 CFR § 1010.520.

---

[2] Remote Deposit Capture allows financial institution customers to "deposit" checks electronically at remote locations, usually in the customers' offices, for virtually instant credit to their account. Paper checks are digitally scanned, and an image of the check is electronically transmitted to the customer's bank.

[3] In civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose. North Dade admits to "willfulness" only as the term is used in civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321(a)(1).

A. Violations of the Requirement to Implement an Anti-Money Laundering Program

North Dade failed to establish and implement an effective anti-money laundering compliance program. The BSA and its implementing regulations require all federally chartered credit unions to establish and implement anti-money laundering programs. 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210. NCUA requires each federally chartered credit union to develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements of the BSA, including an appropriate customer identification program. 12 C.F.R. § 748.2(b); 31 C.F.R. § 1020.220(a)(1).

North Dade failed to establish and maintain an adequate written compliance program that, at a minimum: (1) provided for a system of internal controls to assure ongoing compliance; (2) provided for independent testing for compliance to be conducted by bank personnel or by an outside party; (3) designated an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provided training for appropriate personnel. 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade's compliance program also did not include a customer identification program that was appropriate for its size and type of business. 31 U.S.C. § 5318(l); 31 C.F.R. § 1020.220(a)(1); 12 C.F.R. § 748.2(b)(2).

1. Internal Controls

North Dade failed to implement an effective system of internal controls reasonably designed to ensure compliance with the BSA. It did not timely assess its own money laundering and terrorist financing risks or design an anti-money laundering compliance program to address those risks. As a result, North Dade served a large number of high-risk MSBs outside of its field of membership without exercising adequate compliance oversight.

Risk Assessment

North Dade did not perform a risk assessment until November 2013. A risk assessment is a vital part of a compliance program, as it permits the financial institution to assess its particular risks given its business lines, practices, and clientele and design a program that can reasonably assure and monitor BSA compliance given those risks. North Dade failed to assess the risks of its business lines between December 2009 and November 2013. When NCUA examiners requested a copy of North Dade's risk assessment for its December 31, 2011 exam, they were provided with an outdated template from the 2006 Federal Financial Institutions Examination Council Manual rather than an assessment of North Dade's particular risks. While North Dade had independent audits that identified money laundering and terrorist financing risks in 2012, it did not complete a risk assessment until November 2013. Because North Dade did not examine the services it provided and evaluate the money laundering and terrorist financing risks presented by those services, given North Dade's location, customers, services offered, size, and volume of business, North Dade was ill-equipped to develop a compliance program that included appropriate processes and procedures to address those specific risks and identify suspicious activity.

Risk-Based Procedures to Ensure Compliance

North Dade had insufficient internal controls to identify and monitor suspicious activity taking place through the credit union, in part because it did not assess its own risks and implement procedures designed to address those unique risks. This internal control failure was particularly evident in its generally higher-risk MSB business lines. The most significant example of North Dade's failure to have adequate internal controls and an adequate compliance program is its MSB contract with a third-party vendor.

In December 2009, North Dade entered into a contract with a third-party vendor ("the Vendor"), itself an MSB, to provide financial services to other MSBs, including check-cashing stores and currency exchangers. North Dade agreed to become the depository institution for the Vendor's MSB clients, providing sub-accounts for each MSB to conduct deposits and transfer funds. Under the contract, the Vendor was North Dade's member and customer and the Vendor's MSB clients were not. However, in practice, 56 of the Vendor's MSBs sub-accounts could receive financial services directly from North Dade. In either case, North Dade had anti-money laundering compliance responsibilities with which it did not comply. For example, North Dade's own counsel advised that, although it could open this type of account, North Dade would still have anti-money laundering compliance responsibilities for the Vendor's MSBs. These responsibilities included a customer identification program and other required due diligence on the MSBs and their transactions. Likewise, to the extent opening accounts gave North Dade a direct relationship with the Vendor's MSBs, North Dade would have the same anti-money laundering obligations as it would for any member.

The revenue generated by this business line was vital to North Dade's survival. At one point, the Vendor's MSBs accounted for 90% of North Dade's total annual revenue. The substantial revenue generated by the Vendor's program appeared to outweigh any consideration by North Dade of associated risks and appropriate compliance measures. For example, NCUA examined North Dade in 2010 and instructed the credit union to ensure that its MSB members all met field of membership requirements. But, by December 2012, North Dade had accounts for 56 different MSBs under its Vendor contract that were located outside of North Dade's field of membership. Many of these MSBs were located in jurisdictions in the Middle East and Central America that pose a significant money laundering risk. In addition, despite acknowledging that

it had anti-money laundering compliance responsibilities for these high-risk accounts, North Dade relied on the Vendor to conduct all related due diligence and suspicious activity monitoring without conducting any verification or inspection of the Vendor's compliance activities. Further, North Dade did not verify the customer identification information on the MSBs that the Vendor provided to North Dade.

North Dade did not have sufficient policies and procedures to ensure compliance. Until it instituted a new anti-money laundering policy in November 2013, it lacked: (1) written procedures for opening accounts for members who did not have a social security or tax identification number; (2) written procedures to follow up with account holders whose files were missing social security or tax identification numbers; (3) procedures to ensure that potential high-risk accounts were properly rated as to their money laundering risk; (4) adequate procedures for monitoring accounts for both particular incidents as well as ongoing patterns of suspicious activity; and (5) procedures to retain supporting documentation for filed suspicious activity reports and copies of currency transaction reports.

North Dade's five-person staff did not have sufficient resources or technical expertise to administer a program capable of ensuring compliance with the BSA. North Dade lacked sufficient numbers and expertise in its staff and an adequate technical infrastructure to create, implement, and maintain an anti-money laundering program sufficient to monitor and report on high-volume, high-risk business lines and customers, such as some of the MSBs in the Vendor's contract. As discussed below, North Dade did not provide sufficient training to ensure that its staff had the skills necessary to administer a program to monitor a large number of high-risk customers and transactions, and did not timely obtain the outside assistance or technical resources to compensate for its small staff.

North Dade also did not implement appropriate procedures to manage its customers' compliance risk, given that many of the Vendor's MSBs engaged in particularly high-risk activities, including high-risk currency exchanges. North Dade handled large international transactions for the MSBs. For example, these transactions included, during a one-year period, (1) deposits in excess of $14 million in U.S. cash that was physically imported into the United States on behalf of nearly 40 Mexican currency exchangers, and (2) hundreds of millions of dollars in wire transfers to foreign bank accounts of MSBs located in Mexico and Israel.

Despite these high-risk activities, North Dade did not have any risk or transaction tracking criteria or other compliance procedures to identify and manage high-risk accounts and transactions and instead improperly relied upon the Vendor's compliance activities. For example, one individual, connected to over 60% of the businesses banking with North Dade, conducted transactions between January 2010 and August 2013, that resulted in 2,036 currency transaction reports being filed for cash withdrawals. However, North Dade never identified this customer as being potentially high-risk or reviewed his activities. Because North Dade did not have appropriate policies and procedures in place to identify and monitor high-risk customers and services, numerous suspicious transactions flowed through North Dade accounts without North Dade reviewing them and, when appropriate, filing suspicious activity reports. These suspicious transactions, based on available information, potentially involved money laundering, evasions of Mexican currency transaction restrictions, and drug trafficking.

North Dade failed to have an effective suspicious activity monitoring system for its customers, particularly the Vendor's MSB customers. North Dade relied completely on the Vendor to monitor its MSBs' transactions. In addition, North Dade had insufficient procedures in place to detect suspicious activity among its member customers in general until sometime after

its audit report in August 2013. That report detailed North Dade's inadequate suspicious transaction monitoring procedures and automated systems. In order to monitor for suspicious activities, employees had to manually investigate accounts. However, North Dade's small number of employees lacked the BSA experience, knowledge, and skills to conduct such monitoring, there was an insufficient number of staff to manually review the volume of transactions North Dade was conducting, and North Dade did not implement an appropriate training program to help mitigate this problem. Because of North Dade's failure to appropriately monitor transactions and file SARs for several years, suspicious activity may have gone unnoticed and unreported.

North Dade also did not fully implement the internal controls it did have to ensure BSA compliance. In addition to the Vendor's MSBs, North Dade provided banking services to other MSBs. North Dade's internal policy required each MSB to be properly registered with FinCEN and properly licensed with the state in which they are conducting businesses. In the event that the MSB was not properly registered and licensed, North Dade's written policy was to deny further services to that member. Despite this policy, North Dade continued to provide services to MSBs located in the Middle East, well outside its field of membership, that were not registered with FinCEN.

North Dade failed to assess its money laundering and terrorist financing risks, design appropriate policies and procedures to ensure BSA compliance given those risks, identify customers and monitor their account activities given the customer's level of money laundering risk, and monitor for both individual incidents and ongoing patterns of suspicious activity. North Dade's compliance program was therefore not reasonably designed to ensure BSA compliance.

2. Designation of BSA Compliance Officer

A federally chartered credit union is required to designate a person responsible for ensuring day to day compliance with BSA requirements. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade failed to designate a person responsible to oversee BSA compliance, and no staff member was otherwise assigned or technically competent to oversee ongoing compliance efforts. This compliance violation was highlighted during an independent testing review conducted in 2011. While North Dade repeatedly indicated that it would correct this issue, it failed to designate a compliance officer until January 2014, three years later.

3. Training

A federally chartered credit union's anti-money laundering program must provide for education and training of personnel regarding its responsibilities under the program, including the detection of suspicious transactions. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). North Dade did not have any records of BSA and anti-money laundering compliance for its Board of Directors as recommended by the Federal Financial Institutions Examination Council Manual. North Dade's employees did receive annual BSA training. The training provided, however, was significantly deficient because it (1) did not encompass all aspects of BSA; (2) was not tailored for each department; (3) did not provide sufficient references to external sources to ensure that employees had access to current information on BSA compliance rules and guidance; and (4) did not cover compliance for MSB customers and accounts. Because the training omitted information on MSB compliance and risks, North Dade staff did not have guidance to understand the risks associated with the credit union's largest volume of transactions or how to adequately monitor them.

4. Independent Testing

A federally chartered credit union's anti-money laundering program must include independent compliance testing to monitor the institution's program and ensure its adequacy. 31 C.F.R. § 1020.210; 12 C.F.R. § 748.2(c). NCUA recommends annual testing of a credit union's compliance program when it serves high-risk clients. North Dade did not have its anti-money laundering program tested on a regular basis until NCUA cited this shortfall, a failure of particular concern for an entity, like North Dade, engaged in high-risk business lines. North Dade began receiving independent audits in December 2011 and began addressing some of the programmatic deficiencies shortly thereafter. However, many significant issues persisted almost two years later. North Dade's August 2013 independent audit identified a number of continuing deficiencies, including inadequate suspicious activity monitoring, failing to file timely suspicious activity and currency transaction reports, maintaining accounts for MSBs located outside of North Dade's field of membership, and failing to have procedures to ensure that all required due diligence is performed when new accounts are opened.

B. Customer Identification Program

As part of its anti-money laundering compliance program, a credit union must implement a written Customer Identification Program ("CIP") appropriate for its size and type of business. The program must include risk-based identity verification, recordkeeping, and retention procedures, as well as procedures to determine whether an account is being opened for a government-designated terrorist or terrorist organization and to take appropriate follow-up action if a customer is designated. 31 U.S.C. § 5318(l); 31 C.F.R §§ 1020.210, 1020.220; 12 C.F.R. § 748.2(b)(2). CIP helps a financial institution determine the risks posed by a particular customer, allowing the institution to ensure that it has the proper controls in place, including

suspicious activity monitoring procedures, and to monitor and report on the risks of a particular client.

In relation to the Vendor's MSB clients, North Dade had no procedures in place to address CIP requirements. While North Dade management discussed the high risk posed by this business line as early as March 2010, North Dade's staff and management never reviewed, researched, or verified the identities of the holders of any of the MSB accounts. Instead, North Dade relied exclusively on the Vendor to perform CIP functions. A credit union may rely on another financial institution only in instances where the credit union and the financial institution share customers, and the financial institution is regulated by a federal functional regulator. 31 C.F.R. § 1020.220(a)(6).[4] In this case, North Dade should not have relied on the Vendor for CIP compliance because, as an MSB, the Vendor was not regulated by a federal functional regulator. By not knowing its members, North Dade was not capable of understanding their expected transactional behavior and thus was unable to appropriately monitor for suspicious activities.

C. <u>Suspicious Activity Reporting Violations</u>

The Bank Secrecy Act and its implementing regulations impose an obligation on financial institutions to report transactions that involve or aggregate to at least $5,000; are conducted by, at, or through the financial institution; and that the institution "knows, suspects, or has reason to suspect" are suspicious. 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320(a)(2). A transaction is "suspicious" if the transaction: (1) involves funds derived from illegal activities,

---

[4] See also *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act,* Financial Crimes Enforcement Network, et al. (April 28, 2005), available at http://www.fincen.gov/statutes_regs/guidance/pdf/faqsfinalciprule.pdf.

or is conducted to disguise funds derived from illegal activities; (2) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations under the BSA; or (3) has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction. 31 C.F.R. § 1020.320(a)(2). North Dade failed to detect and timely report suspicious activity.

Between April 2010 and April 2013, North Dade filed only 15 Suspicious Activity Reports ("SARs"). The SARs were filed late and the narrative sections lacked essential information explaining why the suspicious activity was being reported. Furthermore, North Dade failed to file SARs on customers engaged in suspicious activity, including a customer that was arrested and charged with conspiring to launder money. Law enforcement seized more than $1.5 million dollars from an owner of an MSB who held an account at North Dade, yet North Dade never filed a SAR on the MSB or its owner.

D. Section 314(a) of the USA PATRIOT Act

Section 314(a) of the USA PATRIOT Act and its implementing regulations authorize a federal law enforcement agency investigating terrorist activity or money laundering to request that FinCEN solicit, on the agency's behalf, certain information from financial institutions regarding subjects of interest in bona fide law enforcement investigations. Financial institutions are required to review and respond as appropriate to requests from FinCEN on behalf of law enforcement for information relating to individuals, entities, or organizations engaged in, or reasonably suspected based on credible evidence of engaging in, terrorist activity or money laundering. Upon receiving an information request from FinCEN under this section, a financial

institution must expeditiously search its records to determine whether it maintains or has maintained an account for, or has engaged in a transaction with, each individual, entity, or organization named in the request. The 314(a) process provides an important expedited communication system that allows law enforcement to rapidly obtain and evaluate potential lead information in significant and often time-sensitive money laundering and terrorist financing investigations. 31 C.F.R. § 1010.520.[5]

North Dade failed to comply with its Section 314(a) obligations by failing to access or review FinCEN's 314(a) lists from 2012 through 2013. The lists are posted by FinCEN on a secure website every two weeks and must be downloaded and responses verified by the financial institution within a specified deadline. During 2012, the North Dade did not review the list on fourteen of the posted requests and reviewed five requests late. In addition, North Dade had the 314(a) requests sent to a single email address that was accessed by only one person, making timely responses dependent on that person's availability.

III. CIVIL MONEY PENALTY

FinCEN has determined that North Dade willfully violated the program, reporting, and recordkeeping requirements of the Bank Secrecy Act and its implementing regulations, as described in this ASSESSMENT, and that grounds exist to assess a civil money penalty for these violations. 31 U.S.C. § 5321 and 31 C.F.R. § 1010.820. FinCEN has determined that the penalty in this matter will be $300,000.

---

[5] *See also Fincen's 314(a) Fact Sheet* (August 19, 2014), available at http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

IV. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, North Dade consents to the assessment of a civil money penalty in the sum of $300,000, and admits that it violated the BSA's program, recordkeeping, reporting and requirements.

North Dade 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 North Dade to enter into the CONSENT, except for those specified in the CONSENT.

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

V. RELEASE

Execution of the CONSENT, and compliance with all of the terms of this ASSESSMENT and the CONSENT, settles all claims that FinCEN may have against North Dade for the conduct described in Section II of the CONSENT. Execution of the CONSENT, and compliance with the terms of this ASSESSMENT and the CONSENT, does not release any claim that FinCEN may have for conduct by North Dade other than the conduct described in Section II of the CONSENT, or any claim that FinCEN may have against any director, officer, owner, employee, or agent of North Dade, or any party other than North Dade. Upon request, North Dade shall truthfully disclose to FinCEN all factual information not protected by a valid claim of attorney-

client privilege or work product doctrine with respect to the conduct of its current or former directors, officers, employees, agents, or others.

BY:

/S/ November 25, 2014

Jennifer Shasky Calvery Date:
Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury