The Banking Law Journal

Established 1889

An A.S. Pratt® PUBLICATION SEPTEMBER 2015

LexisNexis

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:
Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3000

ISBN: 978-0-7698-7878-2 (print)
ISBN: 978-0-7698-8020-4 (eBook)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub.4815)

Editor-in-Chief & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.

For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer. Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258 (phone). Material for publication is welcomed— articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL LexisNexis Matthew Bender, 630 Central Ave, New Providence, NJ 07974.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

Federal and State Regulators Target Compliance Officers—Part II

Betty Santangelo, Gary Stein, Jennifer M. Opheim, Seetha Ramachandran, and Melissa G.R. Goldstein*

In this two-part article, the authors discuss enforcement actions against compliance officers. The first part of the article, which appeared in the July/August 2015 issue of The Banking Law Journal*, detailed the Financial Crimes Enforcement Network $1-million assessment against the former chief compliance officer ("CCO") at MoneyGram International Inc. ("MoneyGram"). This second part of the article continues the discussion of the MoneyGram action, and also discusses Bank Leumi's consent order with the New York State Department of Financial Services, under which the bank admitted engaging in an illegal cross-border scheme to assist U.S. clients in evading federal and state taxes and agreed to take steps to terminate and/or ban specific employees, including its former CCO, from engaging in compliance functions.*

WILLFUL FAILURE TO ENSURE TIMELY FILING OF SARS

The Charging Documents next allege that Haider failed to ensure that MoneyGram fulfilled its obligation to file timely SARs. Specifically, it is alleged that MoneyGram's AML program was structured in such a way that the individuals responsible for filing SARs were not provided with information from the Fraud Department's Consumer Fraud Report database, which identified the outlets that had accumulated excessive numbers of consumer fraud reports. Contrary to guidance Haider purportedly received from external AML compliance consultants, he did not ensure that the Fraud Department shared relevant information with SAR analysts or provide adequate direction to staff on when SARs should be filed relating to fraud. In effect, Haider purportedly allowed an arrangement whereby separate "silos" of information were maintained, thus preventing SAR analysts from obtaining relevant information. As a result, SARs against known high-risk agents/outlets were not filed or were filed significantly late. In addition, many SARs that MoneyGram filed purportedly incorrectly listed the victim of the fraud as the subject of the

* Betty Santangelo, Gary Stein, Jennifer M. Opheim, Seetha Ramachandran, and Melissa G.R. Goldstein are attorneys at Schulte Roth & Zabel LLP. They may be contacted at betty.santangelo@srz.com, gary.stein@srz.com, jennifer.opheim@srz.com, seetha.ramachandran@srz.com, and melissa.goldstein@srz.com, respectively.

SAR and failed to properly identify the known or suspected complicit agent.[1]

The Charging Documents describe multiple specific examples of outlets/agents that should have been the subject of SARs. Among the factors that the government alleges should have triggered the filing of a SAR were the following:

(1) a significant number of consumer fraud reports were filed against the outlet/agent, and there were quantifiable consumer losses;

(2) identification by AML and Fraud Department personnel of the outlet as one likely to have participated in a fraudulent scheme;

(3) receipt of law enforcement subpoenas regarding the outlets/agents;[2]

(4) whether the agent was ultimately convicted of any crimes;[3] and

(5) whether the outlet had been recommended to Haider for termination.

In numerous instances, the Charging Documents allege that MoneyGram failed to file timely SARs identifying particular agents as suspects during Haider's employment at MoneyGram, but purportedly did so with respect to those same agents and outlets after Haider left the company. According to the Charging Documents, "[a]s 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," and, as a result, its law enforcement objectives were frustrated.[4]

FAILURE TO ENSURE PROPER PERFORMANCE OF AUDITS

In addition, although it is not clear why Haider was responsible for conducting the audits, the Charging Documents claim that 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. As alleged in the Charging Documents, under the BSA, AML programs must include "an independent audit function to test [the] program." Specifically, according to the allegations, MoneyGram did not "consistently perform risk-based audits of agents/outlets, even those it had identified as: (1) having accumulated an excessive number of Consumer

---

[1] Assessment ¶¶ 79–83; Compl. ¶¶ 96–100.

[2] Receipt of law enforcement subpoenas is ordinarily not in and of itself a basis for the filing of a SAR.

[3] It is not clear whether MoneyGram would have known whether the agent was ultimately convicted of any crimes at the time a SAR should have been filed.

[4] Assessment ¶¶ 96–108; Compl. ¶¶ 113–26.

Fraud Reports; and/or (2) possessing other high-risk characteristics." In fact, some of the agents/outlets were purportedly not audited "precisely because the agents/outlets were understood to be engaging in fraud," based on the concern that sending audit teams to those outlets would put them in "physical danger." Haider was allegedly aware of this policy. Likewise, as a result of the lack of sharing of information between the Fraud and AML Compliance Departments, MoneyGram purportedly did not consider the number of consumer fraud reports that MoneyGram's agents/outlets had accumulated when determining which agents/outlets to audit. Furthermore, the Charging Documents allege that even the audits MoneyGram did perform were "frequently ineffective" because on-site auditors were purportedly not trained to look for warning signs of fraud and did not conduct adequate AML reviews.[5]

Relief Sought

Under the BSA, any financial institution and any "partner, director, officer, or employee" of any such financial 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."[6] As alleged in the Charging Documents, "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," including for violations of a financial institution's duty to implement an effective AML program and to timely file SARs.[7] FinCEN may also seek injunctive relief against a person it believes "has violated, is violating, or will violate" the BSA.[8]

Pursuant to that authority, as a result of the alleged failures discussed above, FinCEN's Assessment seeks $1 million from Haider[9] for an assessment period

---

[5] Assessment ¶¶ 6, 86, 88, 90–91; Compl. ¶¶ 16, 103, 105, 107–08.

[6] 31 U.S.C. § 5321(a)(1).

[7] *See id.*; *id.* § 5318(h)(1) ("In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs[.]"); *id.* § 5318(g)(1) ("The Secretary may 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.").

[8] *Id.* § 5320.

[9] The complaint describes this amount as a discount from the $4,750,000 it could have assessed against him. Compl. ¶ 67. According to FinCEN, under the BSA and its implementing regulations, Haider, as an individual responsible for MoneyGram's failure to comply with its AML obligations, is liable for: (1) $25,000 for each day that MoneyGram lacked an effective AML program; and (2) no less than $25,000 (and up to $100,000) for each instance in which the company failed to file a required SAR. Assessment ¶ 6; Compl. ¶ 67.

of 190 days,[10] and the U.S. Attorney's Office is seeking an order: (1) reducing that assessment to a judgment; and (2) "enjoining Haider from participating, directly or indirectly, in the conduct of the affairs of any 'financial institution' (as that term is used in the BSA and its implementing regulations) that is located in the United States or conducts business within the United States, for a term of years—to be determined at trial—sufficient to prevent future harm to the public."[11]

BANK LEUMI DFS CONSENT ORDER

The December 22, 2014 consent order between Bank Leumi[12] and the DFS ("Consent Order") represents another example of an enforcement action aimed specifically at a CCO.[13] In the Consent Order, Bank Leumi admitted that "[f]rom at least 2000 through 2011, it operated a wrongful cross-border banking business that knowingly and willfully aided and assisted U.S. clients, including New York clients, in opening and maintaining undeclared accounts in a foreign country, concealing their offshore assets and income from the Internal Revenue Service and other federal and state authorities, and filing false tax returns and other documents with such authorities."[14] Bank Leumi admitted that in furtherance of that scheme:

- Bank Leumi-Israel and other foreign affiliates "regularly sent private bankers to the United States, including to New York," and, in connection with those visits:

---

[10] FinCEN and Haider entered into tolling agreements, pursuant to which the parties agreed that any statute of limitations applicable here would be tolled from and including Nov. 15, 2103, through and including Dec. 19, 2014. Accordingly, FinCEN based its assessment against Haider on conduct occurring between November 15, 2007 and May 23, 2008 (the date of Haider's separation from MoneyGram). Compl. ¶¶ 65–67.

[11] Compl. ¶ 2.

[12] Bank Leumi-Israel, one of Israel's largest banks with a subsidiary in the United States and an agency in New York, provides private banking, wealth management and other financial services to individuals and entities around the world, including in the United States and New York. Consent Order at 1.

[13] This is not the first time the DFS has specifically sought sanctions against a compliance officer. In June 2014, the DFS entered into a Consent Order with BNP Paribas S.A. ("BNP"), pursuant to which BNP represented that it had fired, among others, the former Group Head of Compliance and the former Head of Ethics and Compliance North America and agreed, as part of its settlement, that it would "not in the future, directly or indirectly, retain" either individual, "as either an officer, employee, agent, consultant, contractor of [BNP], or any affiliate . . . in any other capacity." *See In the Matter of BNP Paribas, S.A.*, DFS Administrative Proceeding, at ¶¶ 57–58 (June 30, 2014), *available at* http://www.dfs.ny.gov/about/ea/ea140630.pdf.

[14] Consent Order ¶ 1.

(1) falsely claimed upon entering the United States that the primary purpose of the bankers' visits were not business-related;

(2) met with prospective customers to discuss opening accounts;

(3) met with existing customers to discuss their undeclared accounts held abroad; and

(4) brought bank statements to the United States for review by U.S. clients;[15] and

- Bank Leumi-Israel assisted clients in concealing accounts through the use of:

  (1) "hold mail" accounts;

  (2) "assumed name" and "numbered" accounts;

  (3) referrals of U.S. clients to outside lawyers and consultants who would establish offshore corporations to hold the undeclared accounts; and

  (4) suggestions to U.S. clients that they open accounts through Bank Leumi Trust to add an "extra level of secrecy" to the account.[16]

According to the Consent Order, Bank Leumi USA assisted in the scheme in at least two ways. First, Bank Leumi USA introduced Bank Leumi-Luxembourg executives to a U.S. tax return preparer who had clients who wanted to open undeclared accounts. Second, it assisted U.S. clients by providing them with loan products that enabled the clients to access their undeclared funds and until 2011 did not identify the U.S. taxpayer who applied for such loans on the loan paperwork.[17]

The Consent Order also criticizes Bank Leumi for soliciting customers of exiting Swiss banks and customers of other foreign banks who had been the subject of cease-and-desist orders for violations of the BSA and AML regulations.[18]

Of particular interest here, Bank Leumi agreed under the Consent Order, among other things, to pay a substantial monetary penalty, retain an independent monitor and take specified actions against certain of its employees,

---

[15] Consent Order ¶ 2.

[16] Consent Order ¶ 3.

[17] Consent Order ¶¶ 4-17.

[18] Consent Order ¶¶ 18–19.

including Bank Leumi USA's former CCO in the United States, as well as individuals located outside the United States.[19] The action by the DFS against the CCO, under which that person cannot "assume any duties, responsibilities, or activities while employed at the Bank that involve compliance in any way," seems to have been motivated by two factors. First, before being appointed as CCO in 2008, the individual had no compliance experience. Second, also in 2008, the CCO was responsible for permitting a policy whereby the Bank "continued to accept and maintain files in the United States that did not contain customer names, so long as the foreign affiliates maintained applicant names and current KYC information in their files." Bank Leumi briefly implemented a policy change that would have required loan documentation to include the applicant's full name and address. After pushback from customers and "extensive internal discussions," Bank Leumi USA's CCO rescinded the policy change in conformance with the request of the foreign affiliate.[20]

CONCLUSION

Although it remains to be seen whether FinCEN and the U.S. Attorney's Office for the Southern District of New York will be able to prove what they have alleged in the Haider action, there are lessons to be learned from that action, as well as the Bank Leumi enforcement action:

- AML Compliance departments should have access to all sources of information that might reveal fraud or money laundering concerns. Law enforcement agencies will look critically upon companies that are structured such that information is "siloed" and not shared with compliance departments, particularly with the individuals in those departments who are responsible for filing SARs. As indicated above in the MoneyGram case, FinCEN is highly critical of such arrangements.[21]

---

[19] Bank Leumi was also required to terminate the current Head of Bank Leumi Trust, who served as Regional Manager during the relevant time period or, if that is not permissible under Israel law, ensure that that employee "shall not be allowed to hold or assume any duties, responsibilities, or activities involving compliance or any matter relating to U.S. operations." Consent Order ¶ 28. Moreover, the Consent Order states that the DFS's investigation resulted in the resignation of a former Branch Manager and Senior Relationship Manager, both of whom "played a central role in the improper conduct discussed in [the] Order." *Id.* ¶ 29.

[20] Consent Order ¶¶ 14, 22, 27.

[21] In a recent advisory, FinCEN advised companies to develop a "culture of compliance," one hallmark of which is that relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts. *See* FIN-2014-A007, "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (Aug. 11,

- AML Compliance personnel may be targeted for enforcement action even in instances where they did not participate in the underlying fraud or money laundering conduct. As noted in the MoneyGram case, they can be targeted for being the architect of a program that is viewed as having deficiencies or for failing to cause the institution to file SARs in a timely manner.
- Although somewhat obvious, companies should make sure that compliance personnel, including AML officers, are qualified to fulfill their responsibilities. Companies should not, for example, place an individual in the position of CCO if that individual does not have any prior compliance experience, as was allegedly the case in the Bank Leumi matter.
- When presented with evidence of potentially fraudulent or illegal conduct passing through one's company, and a decision is made not to take certain steps—particularly steps that are recommended by other company personnel or outside consultants—compliance personnel should document their rationale for declining to take those steps in order to justify their actions years later. In MoneyGram, Haider was apparently unable to explain to FinCEN's satisfaction why he had not terminated certain outlets, apparently lacking a written record as to why those decisions had been made notwithstanding the Fraud Department's recommendations that the outlets should be terminated.

Compliance officers should take steps to ensure that their companies do not bow to pressure from foreign affiliates to engage in conduct that is not permitted in the United States (as in the Bank Leumi case) or to take on business, agents or clients that have been rejected by other companies (as was the case in the MoneyGram matter), particularly where the rejection is potentially connected to alleged fraudulent or money laundering activities.

2014), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf.