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

IN THE MATTER OF:	**)**	
	)	
	)	
	)	**Number 2016-01**
Gibraltar Private Bank and Trust Company	**)**	
Coral Gables, 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 Gibraltar Private Bank and Trust Company ("Gibraltar" or the "Bank"), pursuant to the Bank Secrecy Act ("BSA") and regulations issued pursuant to that Act.[1]

Gibraltar admits to the facts set forth below and that its conduct violated the BSA.[2] Gibraltar consented to the assessment of a civil money penalty and entered into the CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY ("CONSENT") with FinCEN.

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

[2] Gibraltar makes the admissions as stated above and elsewhere in this document solely in connection with the resolution of this civil proceeding and for purposes of the imposition of the civil penalty set forth herein. Nothing in the CONSENT, including Paragraph VI, will be construed by FinCEN to prevent Gibraltar or its agents from offering a defense (including denials of related factual allegations made by other government agencies or in litigation) in any litigation or government investigation, so long as the statement, defense, or argument is made (1) to a government investigative agency; or (2) to a court, in writing or orally; or (3) in any sworn testimony in connection with a judicial or administrative proceeding.

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

FinCEN has the authority to investigate banks for compliance with and violation 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. . . ."

Gibraltar was a "financial institution" and a "bank" within the meaning of the BSA and its implementing regulations during the time relevant to this action.[3]

Gibraltar is a community bank headquartered in Coral Gables, Florida, that provides loan, deposit, and other financial services to high net-worth clients. As of December 31, 2015, Gibraltar had approximately $1.57 billion in total assets, with seven offices located in Florida and one office in New York.

Resolution with the Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency ("OCC") succeeded the Office of Thrift Supervision ("OTS") in July 2011 as Gibraltar's primary federal functional regulator, and examines banks, including Gibraltar, for compliance with the BSA and similar rules under Title 12 of the United States Code.[4] In May 2010, OTS conducted an examination of Gibraltar that revealed anti-money laundering program deficiencies resulting in the failure to file numerous suspicious activity reports ("SARs") in a timely, complete, and accurate manner. On October 15, 2010, Gibraltar stipulated to the issuance of a Cease and Desist Order with the OTS ("OTS Order") which required Gibraltar to undertake remedial actions with respect to its BSA compliance program. The OCC

[3] 31 U.S.C. § 5312(a)(2)(A); 31 C.F.R. § 1010.100.

[4] On July 21, 2011, the relevant functions of the OTS were transferred to the OCC.

conducted four subsequent exams on Gibraltar from 2011 through 2014, and continually identified significant deficiencies in Gibraltar's BSA compliance program and customer due diligence and reporting obligations. On October 16, 2014, the OCC replaced the 2010 OTS Order with a Consent Order to further address Gibraltar's BSA program deficiencies.

For these reasons, Gibraltar has agreed to a $2.5 million civil money penalty assessed by the OCC.

II. DETERMINATIONS

Gibraltar willfully violated the BSA's program, reporting, and recordkeeping requirements from February 2008 through October 2014. As described below, Gibraltar failed to (a) implement and maintain an adequate anti-money laundering program, (b) develop and implement an adequate customer identification program, and (c) detect and adequately report suspicious transactions. Gibraltar's substantial program deficiencies led to its failure to monitor and detect suspicious activity despite red flags. These deficiencies ultimately caused Gibraltar to fail to timely file at least 120 suspicious activity reports ("SARs") involving nearly $558 million in transactions occurring during the period of 2009 to 2013, much of which related to a $1.2 billion Ponzi scheme perpetrated by Scott Rothstein, as discussed further below.[5]

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

[5] 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. Gibraltar admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).

Gibraltar failed to establish and implement an effective anti-money laundering compliance program as required by the BSA and its implementing regulations.[6] The OCC requires each bank under its supervision to develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the BSA's recordkeeping and reporting requirements, including an appropriate customer identification program.[7] At a minimum, a bank's anti-money laundering compliance program must: (a) provide for a system of internal controls to assure ongoing compliance; (b) provide for independent testing for compliance to be conducted by bank personnel or by an outside party; (c) designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (d) provide training for appropriate personnel.[8]

Gibraltar failed to establish and maintain adequate internal controls to assure ongoing compliance and it did not provide adequate training for appropriate personnel.[9] Gibraltar's anti-money laundering compliance program also did not include a customer identification program that was appropriate for its size and type of business.[10]

1. Internal Controls

Gibraltar failed to implement an effective system of internal controls reasonably designed to ensure compliance with the BSA.[11] It did not adequately monitor, detect, or report suspicious activity. It further failed to assess its money laundering risks and design an effective anti-money

[6] 31 U.S.C. §§ 5318(a)(2), 5318(h); 31 C.F.R. § 1020.210.

[7] 12 C.F.R. § 21.21

[8] 31 U.S.C. §§ 5318(a)(2), 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 21.21.

[9] 31 U.S.C. §§ 5318(a)(2), 5318(h)(1); 31 C.F.R. § 1020.210; 12 C.F.R. § 21.21.

[10] 31 C.F.R. § 1020.220.

[11] 31 U.S.C. § 5318(h)(1)(A); 31 C.F.R. § 1020.210.

laundering compliance program to address those risks. As a result, Gibraltar serviced high-risk customers without effectively monitoring their respective accounts, and failed to detect and report suspicious activities in a timely manner.

a. Transaction Monitoring.

Gibraltar's procedures for monitoring, detecting, and reporting suspicious activity were ineffective. Banks are required to implement transaction monitoring procedures and file reports of suspicious activity with FinCEN. Like other BSA filings, SARs play an important role in detecting possible criminal activity. FinCEN and law enforcement agencies use SARs to investigate money laundering, terrorist financing, and other serious criminal activity. Although Gibraltar used a software system to monitor its accounts for unusual activity going through the Bank, the system and procedures were so flawed, that Gibraltar systematically failed to identify and timely report transactions through numerous accounts that exhibited indicia of money laundering or other suspicious activity.

Several factors contributed to Gibraltar's ineffective transaction monitoring system that remained deficient from at least 2008 through 2014. First, Gibraltar's transaction monitoring system contained account opening information and customer risk profiles that were frequently incomplete, inaccurate, and lacked sufficient analysis and validation. In addition, the anticipated account activity for some customers often did not match the actual transaction activity. Because of the incomplete and inaccurate information, when the Bank's automated transaction monitoring system generated alerts on certain customers, analysts in the BSA department could not determine effectively when a change in those customers' activities should have resulted in a change to those customers' risk ratings.

Second, Gibraltar's automated monitoring system deficiencies resulted in its generation of an unmanageable number of alerts that included large numbers of false positives. Significantly, OTS examiners first highlighted the inefficiency of Gibraltar's monitoring system as early as 2010,

but it was not fully rectified until mid-2014. The problems associated with the system were due to Gibraltar's failure to adequately tailor the parameters and thresholds of the alerts generated by the system to match the high-risk activities it sought to identify and control. Also contributing to this deficiency was that prior to 2013, Gibraltar did not validate or independently test the system's parameters and thresholds to reduce the number of false positive alerts the system generated. Consequently, Gibraltar's failure to accurately set, validate, and test the automated monitoring system left Gibraltar overwhelmed by the large volume of alerts, many of which yielded false positive results.

Hampered by a large volume, Gibraltar's BSA analysts were also unable to timely or adequately review or investigate all of the alerts. For example, from early August 2013 to late July 2014, Gibraltar failed to review and close or escalate nearly 60% of its monthly alerts in the 30 days prescribed by Gibraltar's own BSA/AML policy. When Gibraltar did review alerts, there were numerous instances when Gibraltar closed alerts that should have been escalated. And, in those instances where alerts were escalated to investigations for potential SAR filings, 16 alerts, or 64% of the escalated reviews, took over 60 days to escalate for further investigation. Eleven of these reviews resulted in SAR filings.

The aforementioned deficiencies over the course of several years contributed to a monitoring process, which took too long to review and report potentially suspicious activity. In just one instance, between February 2008 and December 2009, Gibraltar processed approximately $790,000 in wires to a foreign country on behalf of a customer, which substantially deviated from the customer's expected activity at the time the account was opened. Gibraltar risk-rated the account as low risk, which required Gibraltar to review the account for suspicious activity after its system generated three alerts for suspicious activity. Gibraltar's suspicious activity monitoring system

generated three alerts for this account during the last quarter of 2009. However, Gibraltar did not initiate a review of the account until May 2010, and it did not file a SAR regarding the activity until July 2010 – seven months after the last alert. In addition, as described in more detail below, Gibraltar's failure to adequately monitor for suspicious activity resulted in its failure to timely file at least 120 SARs.

The deficiencies of Gibraltar's SAR reporting were also due in part to Gibraltar's investigation process. For example, Gibraltar's BSA Officer in 2009 and 2010 spent approximately two years, an unreasonable amount of time given the information the Bank had, investigating relationships and transactions related to Scott Rothstein, a partner in the law firm of Rothstein, Rosenfeld, and Adler, PA (RRA). As further discussed below, Rothstein led a $1.2 billion Ponzi scheme for which he was convicted on Racketeer Influenced and Corrupt Organizations Act (RICO) conspiracy charges and sentenced to 50 years in a federal prison. For approximately two years, the former BSA Officer and the Rothstein account officer unsuccessfully attempted to get information from Rothstein to determine the legitimacy of his transactions. However, within nine months of the investigation, the former BSA Officer received two other suspicious activity referrals from other bank officers for the Rothstein accounts. At this point, based on multiple instances of significant suspicious activity coupled with Rothstein's lack of cooperation, the former BSA Officer should have escalated the investigation and filed a SAR. However, Gibraltar allowed the investigation to languish and did not file a suspicious activity report on Rothstein-related activities until after information regarding Rothstein's activities appeared in the media.

b. Risk Assessment.

Gibraltar also failed to adequately assess the money laundering risks associated with its customers. Risk assessment procedures are a key component of a compliance program because they

permit a financial institution to assess its particular risks associated with its business lines, practices, and clientele and to design a program that can reasonably assure and monitor BSA compliance. While Gibraltar undertook several AML risk assessments between February 2008 and October 2014, Gibraltar failed to adequately risk rate its high-risk customers and their respective accounts, leaving the Bank ill-equipped to adequately monitor transactions based on a customer's particular level of risk or the account's purpose and expected activity. Moreover, on some occasions, when Gibraltar detected a deviation in a customer's activity from anticipated activity identified at account opening, it would change the anticipated activity in the account rather than changing customer's risk rating, even when the customer should have been identified as high risk. This practice undermined the purpose of conducting risk ratings and caused Gibraltar to apply insufficient transaction monitoring to accounts it should have identified as high-risk and limited Gibraltar's ability to detect red flags of suspicious activity.

For example, Gibraltar did not adequately risk rate its high net-worth private banking customers, like Scott Rothstein. As a result, the Bank applied insufficient scrutiny to his and related accounts, and missed the following significant red flags.

- Rothstein used his account to conduct millions of dollars of intrabank and interbank funds transfers sent in large, round-dollar amounts. The continued movement of large round-dollar amounts within accounts at the same institution is red flag activity indicative of a Ponzi scheme.
- The account also processed unexplained funds transfer activity and payments and receipts with no links to legitimate services provided. The Bank should have identified that this activity was not expected for the Rothstein accounts and, as unexpected activity, should have investigated it further.

- A significant volume of highly suspicious transactional activity involved multiple Interest on Trust Accounts ("IOTAs") controlled by Rothstein that did not match his customer information file. An IOTA is an account set up by an attorney to hold client funds received for future use, and cannot be used to support ongoing transaction activity. Had Gibraltar applied appropriate scrutiny to Rothstein's accounts, it would have identified as suspicious Rothstein's improper use of IOTAs to support his massive Ponzi scheme.

In addition, in 2011, Gibraltar's customer risk profiles were generally incomplete, stale, and lacking in sufficient analysis and validation. Some account files lacked sufficient supporting documentation to validate the risk profiles of the beneficial owners or authorized signers. Such files also were generally missing descriptions regarding the source of funds, financial capacity, expected activity, and the purpose of the account. By failing to have complete and accurate information, Gibraltar was unable to accurately risk rate such accounts either at account opening or when updating its account risk ratings. Further, when updating its account risk ratings, rather than soliciting updated and more accurate information from customers to conduct a comprehensive assessment, Gibraltar would simply review its account risk ratings based on average account activity that the Bank did not validate with the customer's expected activity.

In 2013, the risk rating methodology of all deposit accounts was also considered deficient. The methodology did not consider the volume of customer activity by transaction type (e.g., cash activity, wire activity, and ACH activity). The type of transaction being used by the account is an important factor in identifying an expected volume of customer activity. This is important because such information is necessary to identify baselines with which to compare actual activity for transaction monitoring.

For over three years, Gibraltar did not have up-to-date, accurate, and verified information to enable it to conduct its annual risk assessment. Gibraltar's information was unreliable because, from 2011 through 2014, it failed to complete a full cycle of annual high-risk account reviews. In fact, in 2014, the Bank had conducted only 44 (or 7%) annual high-risk reviews out of 590 high-risk customer information files.

In sum, Gibraltar's transaction and suspicious activity monitoring deficiencies from 2008 through 2013, combined with its overall risk assessment and risk rating deficiencies, demonstrate Gibraltar's continuous failure to maintain an anti-money laundering compliance program that adequately identified the risks posed by its products, services, customers, and its customers' activities.

2. Training

A bank's anti-money laundering program must provide for education and training of personnel regarding their responsibilities under the program, including monitoring, detecting, and reporting suspicious transactions. [12] Throughout 2009 to 2014, Gibraltar's implementation of BSA training was continually inadequate. It failed to provide appropriate training tailored to the needs of specific positions, departments, board members, and other personnel. For example, in 2009, Gibraltar's senior bank officials had only taken a basic BSA course that was not appropriate for their functional responsibilities, as it was specifically designed for tellers. The Bank's management undertook an assessment in May 2013 of its BSA department's training needs. This assessment indicated that its BSA/AML personnel required significant training in order to adequately implement its BSA/AML compliance program. However, over a year later in 2014, the Bank had still not addressed any of the needs identified in its 2013 assessment.

[12] 31 U.S.C. § 5318(h)(1)(C); 31 C.F.R §§ 1020.210, 1020.220(a)(2)(i).

B. Violation of Requirement to Develop and Implement an Adequate Customer Identification Program

As part of its anti-money laundering compliance program, a bank must implement a written customer identification program appropriate for its size and type of business. The program must include risk-based identity verification, recordkeeping, and retention procedures. In general, the minimum information a bank must obtain prior to opening an account is the customer's name, date of birth, and a residential or business street address. A customer identification program 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.

Gibraltar consistently failed to maintain a sufficient customer identification program from February 2008 through October 2014. Gibraltar's customer due diligence was insufficient to develop accurate risk profiles and to effectively understand its customers' business and predicted activity. For example, Gibraltar opened numerous accounts with missing information and some with no documentation at all. In 2013, the Bank made efforts to obtain, document, and verify sufficient customer information for its customer profiles. However, Gibraltar failed to complete these efforts by failing to obtain information on customers' wealth and expected activity. Also, the Bank failed to identify all related depository and fiduciary accounts and loans. These failures prevented Gibraltar from adequately monitoring account behavior against established customer profiles.

Gibraltar also failed to incorporate its customer identification program into its internal controls, including transaction monitoring. For a customer identification program to be effective, a bank must incorporate customer files into its transaction monitoring processes. In 2013, although the Bank had a procedure to identify accounts by relationship, it did not always comply with that procedure to ensure that all accounts were successfully associated. For example, Gibraltar added

accounts in the Wealth Management area without taking steps to determine if related accounts existed in other areas of the Bank, even though its policies and procedures required it to do so. Consequently, customer information files for related high-risk accounts were often not linked, impairing Gibraltar's ability to identify common information among apparently disparate accounts, recognize common ownership, and treat all related accounts as a single relationship. By not associating these accounts as single relationships, Gibraltar negatively impacted the effectiveness of its transaction monitoring and other internal controls.

As a result of Gibraltar's serious deficiencies involving customer due diligence and customer identification procedures, Gibraltar was unable to detect multiple instances of suspicious activity based on information generated from Gibraltar's due diligence procedures.

C. Violations of the Requirement to Report Suspicious Transactions

Gibraltar failed to adequately report suspicious activity. The BSA and its implementing regulations impose an obligation on banks to report transactions that involve or aggregate to at least $5,000, are conducted by, at, or through the bank, and that the bank "knows, suspects, or has reason to suspect" are suspicious.[13] A transaction is "suspicious" if the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations under the Act; or (c) has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction.[14]

[13] 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

[14] 31 C.F.R. §§ 1020.320(a)(2)(i) - (iii).

As a result of Gibraltar's severely deficient transaction monitoring process described above, Gibraltar failed to properly report suspicious activities related to the transactions conducted on behalf of Scott Rothstein, associated individuals and entities, and their related accounts in a timely manner. Gibraltar ultimately filed over 100 SARs involving millions of dollars in potentially suspicious activity involving Rothstein-related accounts from 2009. Gibraltar reported almost all of this activity well over 60 days from the time that it knew or had reason to know the transactions were suspicious.

Gibraltar also filed late SARs on entities and customers unrelated to Rothstein. These late SARs documented potential mortgage fraud, embezzlement, suspicious wire transfers, corruption, and structuring involving customers unrelated to Rothstein. On a number of occasions, Gibraltar filed SARs late over the course of five years; in some cases, years after the suspicious activity had occurred. For transactions occurring during the period of 2009 to 2013, Gibraltar failed to detect and timely report 120 instances of suspicious activity involving nearly $558 million in suspicious activity, of which $363 million involved accounts related to Scott Rothstein's Ponzi scheme.

III. CIVIL MONEY PENALTY

FinCEN has determined that Gibraltar willfully violated the anti-money laundering program, reporting, and recordkeeping requirements of the BSA and its implementing regulations, as described in the CONSENT. FinCEN has also determined that grounds exist to assess a civil money penalty for these violations.[15]

FinCEN has determined that the penalty in this matter will be $4 million, of which $2.5 million will be concurrent with the penalty imposed by the OCC. Accordingly, this penalty will be

[15] 31 U.S.C. § 5321; 31 C.F.R. § 1010.820.

satisfied by paying $1.5 million to the United States Department of the Treasury and by paying $2.5 million in satisfaction of, and in accordance with, the penalty imposed by the OCC.

IV. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, Gibraltar has consented to this ASSESSMENT of a civil money penalty in the sum of $4 million as described above, and has admitted that it violated the BSA's anti-money laundering program, recordkeeping, and reporting requirements.

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

Gibraltar understands and agrees that the CONSENT embodies the entire agreement between Gibraltar and FinCEN relating to this enforcement matter only, as described in Section II above. Gibraltar further understands and agrees that there are no express or implied promises, representations, or agreements between Gibraltar and FinCEN other than those expressly set forth or referred to in this document and that nothing in the CONSENT or in this ASSESSMENT OF CIVIL MONEY PENALTY ("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 Gibraltar 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 Gibraltar other than the conduct described in Section II of the CONSENT, or any claim that FinCEN may have against parties other than Gibraltar, including, without limitation, any current or former partner, director, officer, or employee of Gibraltar. Upon request, Gibraltar 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.

VI. PUBLIC STATEMENTS CLAUSE

Gibraltar expressly agreed that it shall not, nor shall its attorneys, agents, partners, directors, officer, employees, affiliates, or any other person authorized to speak on its behalf, make any public statement contradicting either its acceptance of responsibility set forth in the CONSENT or any fact in the DETERMINATIONS section of the CONSENT. FinCEN has sole discretion to determine whether a statement is contradictory and violates the terms of the CONSENT. If Gibraltar, or anyone claiming to speak on behalf of Gibraltar makes such a contradictory statement, Gibraltar may avoid a breach of the agreement by repudiating such statement within 48 hours of notification by FinCEN. If FinCEN determines that Gibraltar did not satisfactorily repudiate such statement(s) within 48 hours of notification, FinCEN may void, in its sole discretion, the releases contained in the CONSENT and reinstitute enforcement proceedings against Gibraltar. Gibraltar expressly agreed to waive any statute of limitations defense to the reinstituted enforcement proceedings and further agreed not to contest any admission or other findings made in the DETERMINATIONS section of the CONSENT.

This paragraph does not apply to any statement made by any present or former officer, director, employee, or agent of Gibraltar in the course of any criminal, regulatory, or civil case initiated against such individual, unless Gibraltar later ratifies such claims, directly or

indirectly. Gibraltar further agreed that, upon notification by FinCEN, Gibraltar will repudiate such statement to the extent it contradicts either its acceptance of responsibility or any fact in the DETERMINATIONS section of the CONSENT.

By:

/s/ February 25, 2016

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