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

IN THE MATTER OF:	**)**	
	)	
	)	**Number 2011 - 7**
OCEAN BANK,	**)**	
MIAMI, FLORIDA	**)**	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

Under the authority of the Bank Secrecy Act ("BSA") and regulations issued pursuant to that Act,[1] the Financial Crimes Enforcement Network ("FinCEN") of the Department of the Treasury has determined that grounds exist to assess a civil money penalty against Ocean Bank, Miami, Florida ("Ocean" or "the Bank"). Ocean enters into the CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY ("CONSENT") without admitting or denying the determinations by FinCEN, as described in Sections III and IV below, except as to jurisdiction in Section II below, which is admitted.

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

II. JURISDICTION

Ocean, the largest state chartered bank in Florida, is privately owned and headquartered in Miami. With twenty-one branches located throughout southern Florida, Ocean provides a wide range of financial services to consumers, small businesses and middle-market companies. The Federal Deposit Insurance Corporation ("FDIC") is the Bank's Federal functional regulator and examines the Bank for compliance with the BSA, its implementing regulations and similar rules under Title 12 of the United States Code. Additionally, the Florida Office of Financial Regulation ("FOFR") shares similar responsibilities with the FDIC, including examining Ocean

[1] 31 U.S.C. § 5311 et seq. and 31 C.F.R. Part 103 (31 C.F.R. Chapter X). On March 1, 2011, a transfer and reorganization of Bank Secrecy Act regulations from 31 C.F.R. Part 103 to 31 C.F.R. Chapter X became effective. Throughout this document we cite the Part 103 regulation in effect at the time of the Bank's violation. The Part 103 regulatory citation is followed by the current Chapter X citation in parentheses.

for compliance with the BSA. As of March 31, 2011, Ocean had assets in the amount of approximately $3.6 billion and $2.2 million in net income.

At all relevant times, Ocean was a "financial institution" and a "bank" within the meaning of the BSA and the regulations issued pursuant to that Act.[2]

III. DETERMINATIONS

A. Summary

An investigation conducted by the Drug Enforcement Administration, Internal Revenue Service - Criminal Investigation and FinCEN, working in conjunction with the United States Attorney's Office for the Southern District of Florida, and parallel examinations conducted by the FDIC and the FOFR, determined that from 2005 to 2010, Ocean violated the anti-money laundering ("AML") program requirements, suspicious activity reporting requirements, and currency transaction reporting requirements of the BSA.[3] In July of 2007, the Bank consented to the issuance of a Cease and Desist Order issued by the FDIC relative to non-compliance with the BSA.[4] A modified Consent Order replaced the Cease and Desist Order and remains in effect to this day. Appearing below is a summary of the violations of the BSA by Ocean.

The AML program at Ocean was deficient in three of the four core elements required by 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 103.120 (31 C.F.R. § 1020.210). Namely, the Bank failed to:

- establish and implement effective internal controls;
- designate personnel to ensure day-to-day compliance;
- implement an effective independent audit function to test programs with respect to the BSA, particularly the suspicious activity reporting requirements.

Ocean failed to implement an effective AML program reasonably designed to identify and report transactions that exhibited indicia of money laundering or other suspicious activity, considering the types of products and services offered by the Bank, the volume and scope of its business, and the nature of its customers. Ocean failed to implement a program commensurate with the risks inherent within its business lines and geographical reach. As a result, Ocean failed to timely file suspicious activity reports, thus greatly diminishing the value of the reports to both law enforcement and regulatory agencies.

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

[2] 31 U.S.C. § 5312(a)(2) and 31 C.F.R. § 103.120 (31 C.F.R. § 1020.210).
[3] 31 U.S.C. § 5318(h)(1), 31 C.F.R. § 103.120, 31 C.F.R. § 103.18, and 31 C.F.R. § 103.22 (31 C.F.R. § 1020.210, 31 C.F.R. §1020.320, and 31 C.F.R. §1010.311).
[4] Order to Cease and Desist, FDIC-07-017b, 3/16/07.

FinCEN has determined that Ocean violated the requirement to establish and implement an adequate AML program. Since April 24, 2002, the BSA and its implementing regulations have required banks to establish and implement AML programs.[5] A bank is deemed to have satisfied the requirements of 31 U.S.C. § 5318(h)(1) if it implements and maintains an anti-money laundering program that complies with the regulations of its Federal functional regulator governing such programs.[6] The FDIC requires each bank under its supervision to establish and maintain an AML program that, at a minimum: (1) provides for a system of internal controls to assure ongoing compliance; (2) provides for independent testing for compliance conducted by bank personnel or by an outside party; (3) designates an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provides training for appropriate personnel.[7]

1. Internal Policies, Procedures and Controls

Ocean failed to implement an effective system of internal controls to ensure compliance with the BSA and manage the risks of money laundering. Twenty-eight percent of the Bank's total customers reside outside of the United States in high-risk geographies susceptible to money laundering, including Venezuela. The Bank established direct account relationships in the United States for Politically Exposed Persons ("PEPs"), Consulates and established "bearer share" corporations.

Given the high-risk nature of its account base, Ocean lacked adequate policies, procedures and an effective system of internal controls reasonably designed to assess and mitigate the risks of narcotics-related money laundering activity and ensure the detection and reporting of suspicious transactions.

Venezuela is one of the principal drug-transit countries in the Western Hemisphere. Venezuela's proximity to drug producing countries, weaknesses in its AML regime and alleged corruption continue to make Venezuela vulnerable to money laundering. The main sources of money laundering are proceeds generated by drug trafficking organizations and illegal transactions that exploit Venezuela's currency controls and its various exchange rates.[8]

Generally in Venezuela money laundering occurs through commercial banks, exchange houses, gambling sites, fraudulently invoiced foreign trade transactions, smuggling, real estate (in the tourist industry), agriculture and livestock businesses, securities transactions, and trade in precious metals.[9]

[5] 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 103.120 (31 C.F.R. § 1020.210).
[6] 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 103.120 (31 C.F.R. § 1020.210).
[7] 12 C.F.R. § 326.8(b) and (c).
[8] http://www.state.gov/p/inl/rls/nrcrpt/2011/vol2/156376.htm#venezuela.
[9] Id.

Account opening documents for the Bank's foreign customers arrived in the United States via mail pouch. The Bank did not adequately verify the identity and account opening documents for its foreign customer accounts. Ocean opened accounts for customers in Venezuela without face-to-face contact. Documentation of customer identification was not subject to adequate quality controls to ensure the accuracy of information. The Bank failed to maintain complete and sufficient documentation to develop appropriate customer profiles.

Ocean's policies, procedures and controls failed to ensure that the Bank gathered and reviewed sufficient information on foreign and domestic account customers to adequately assess risk and potential for money laundering. A sampling of both foreign and domestic retail customer files showed errors and omissions in the Bank's documentation of specific customer information, including the nature of the customers' businesses, verification of owner/operator identities, and anticipated account activity. The Bank lacked a clearly defined system for periodically updating customer information or amending expected activity profiles, as necessary, with approval by the BSA Officer or senior management.

The Bank failed to update or conduct periodic reviews of both domestic and foreign customer accounts, and failed to focus sufficient attention on the accounts and transactions that exhibited high-risk characteristics for money laundering. These deficiencies prevented the Bank from performing adequate analysis of the risks, associated with particular customers, to determine whether transactions lacked any apparent business or lawful purpose, or were within the particular customer's normal expected range of conduct.

The Bank failed to structure its BSA/AML compliance program to adequately address the risks of its customer base. Specifically, Ocean failed to implement an adequate risk-rating methodology that evaluated customers, based on specific customer information, with balanced consideration to all relevant factors including country/jurisdictional risk, products and services provided, nature of the customer's business and volume of transactions. Even when the Bank rated certain customers as "high risk," it did not apply commensurate due diligence practices and transaction monitoring.

Ocean lacked adequate systems and controls to monitor transactions conducted by its customers for potential money laundering or other suspicious activity. Ocean failed to readily identify "Red Flags"[10] often associated with suspicious activity involving individual transactions – particularly large round tens of thousands of dollar wire transactions, inconsistent with company profiles and lacking any apparent business or lawful purpose.

In 2003, the Bank implemented an automated account monitoring system. However, only 15 percent of the Bank's total accounts – those classified as "high risk" were covered by the system; leaving more than 97,000 accounts to be monitored manually. Based on the scope,

[10] Bank Secrecy Act Advisory Group, "Section 1 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 7, August 2004, pages 7 – 8.

volume, and magnitude of transaction activity within the accounts, manual processing was not sufficient to ensure compliance with the BSA.

By the end of 2006, a backlog of over 100,000 alerts had been generated by the Bank's monitoring system, even though only 15 percent of the Bank's customer accounts were being monitored automatically. The overwhelming majority of these alerts were subsequently cleared by Bank staff that was ill-trained, inexperienced in reporting suspicious activity and without proper review. Furthermore, the implementation and oversight of an automated monitoring system continued to suffer from inadequacies for years. As a result, few suspicious activity reports were filed by the Bank relative to the number of alerts generated. The Bank eventually cleared its backlog of alerts in 2009.

The Bank's automated monitoring system was ineffective in detecting suspicious activity as appropriate parameters were not established relative to customer risk and anticipated account activity. The Bank failed to properly monitor internal account transfers, Automated Clearing House ("ACH") transactions and check, loan and trade finance transactions. The Bank failed to document or explain account filtering criteria or thresholds, and how both were appropriate for the Bank's risks. The Bank failed to periodically review and update the filtering criteria and thresholds thus rendering them ineffective. The monitoring system's programming, methodology, and effectiveness were not independently validated until 2009, to ensure that the models were detecting potentially suspicious activity. Despite these efforts, the Bank's automated monitoring system continued to be ineffective in identifying suspicious activity.

Ocean failed to implement adequate procedures, systems and internal controls reasonably designed to detect and report possible instances of money laundering relative to foreign high risk customer accounts. Such measures would have enabled Ocean to obtain the requisite information necessary to perform appropriate due diligence on foreign customers and determine whether transactions conducted in the United States were consistent with the customers' normal range or expected range of conduct, or lacked any apparent business or lawful purpose.

As mentioned above, the Bank failed to adequately monitor the transactions of its customers to determine if the actual activity was commensurate with expected activity, and/or lacked any apparent business or lawful purpose. Domestic and foreign account customers received frequent high-value round dollar wires from Mexican Casas de Cambio. One particular customer received high-value round dollar wires from the same Casa de Cambio in multiple transactions on the very same day. Based on the Bank's customer profile, these high-value round dollar wires were received from a location clearly outside of the customer's stated business geography. Because of the Bank's inadequate transaction monitoring systems, such activity was not flagged as being suspicious.

The Bank failed to file timely suspicious activity reports with respect to the receipt and transfer by its customers of tens of millions of dollars in wire transactions. On those occasions

where the Bank filed suspicious activity reports, few were filed within the same year of receipt of such wires. The majority of suspicious activity reports filed by the Bank report activity a year, or in some instances years, after such activity. The resulting delays and incomplete information impaired the usefulness of the suspicious activity reports by not providing law enforcement with more timely and comprehensive information related to millions of dollars in potentially suspicious transactions.

Pursuant to Section 314(a) of the USA PATRIOT Act, FinCEN receives requests from Federal law enforcement and upon review, sends requests to designated contacts within financial institutions across the country once every two weeks via a secure Internet Web site. The requests are in the furtherance of terrorist financing and significant money laundering investigations, and contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records. The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding twelve months and transactions conducted within the last six months. Financial institutions have two weeks from the transmission date of the request to respond to 314(a) requests. Through an expedited communication system FinCEN's 314(a) process enables investigators to canvass the nation's financial institutions for potential lead information that might otherwise never be uncovered.[11]

Deficiencies in Ocean's procedures, systems and internal controls caused the Bank to fail to recognize that for a period of four months in 2006, it did not respond to a number of 314(a) requests from FinCEN.

Additionally, the Bank failed to recognize the importance of law enforcement inquiries and requests. Such inquiries included grand jury subpoenas and National Security Letters ("NSLs"). The receipt of a grand jury subpoena should cause a financial institution to conduct a risk assessment of the subject customer and also review its account activity.[12] Criminal or grand jury subpoenas with any indicia of money laundering and/or specified unlawful activity ("SUA") may lead to the reporting of suspicious activity, which has value to law enforcement authorities outside of the subpoena process.

2. Designation of Compliance Personnel

Ocean failed to adequately staff the BSA compliance function at the Bank with personnel to ensure day-to-day compliance with the BSA. The unit responsible for monitoring the Bank's domestic and foreign retail customer accounts was understaffed, and personnel lacked the requisite knowledge and expertise to adequately perform their duties. The Bank failed to recognize the risks inherent within its retail business lines and failed to provide adequate staffing

[11] FinCEN's 314(a) Factsheet, 6/14/11, http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

[12] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, pages 42 – 44.

to mitigate such risks. The Bank's failure to provide adequate numbers of appropriately trained personnel limited its ability to initiate and complete reviews and file complete, accurate, and timely suspicious activity reports.

3. Independent Testing for Compliance

FinCEN has determined that Ocean's program for independent testing for compliance with the BSA was ineffective and failed to ensure compliance. In view of the inherent risk associated with its customer base, the Bank did not implement an effective independent audit function, in terms of both scope and frequency, to manage the risk of money laundering and compliance with the BSA. The internal audit function did not adequately evaluate and test Ocean's suspicious activity monitoring and reporting systems, the Bank's foreign and domestic customer due diligence program, or other aspects of its AML program.

Audits were not conducted commensurate with the BSA/AML risk profile of the Bank. As a result, the scope and frequency of the independent reviews were insufficient.

C. Violations of the Requirement to Report Suspicious Activity

FinCEN has determined that Ocean violated the suspicious transactions reporting requirements of the BSA and regulations implemented pursuant to that Act. These reporting requirements 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 financial institution "knows, suspects, or has reason to suspect" are suspicious.[13] A transaction is "suspicious" if the transaction: (1) involves funds derived from illegal activities, or is conducted to disguise the funds derived from illegal activities; (2) is designed to evade reporting or record keeping requirements under the Bank Secrecy Act; or (3) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[14]

Financial institutions must report suspicious transactions by filing suspicious activity reports, generally no later than thirty calendar days after detecting the facts that may constitute a basis for filing a suspicious report. If no suspect was identified on the date of detection, a bank may delay the filing for an additional thirty calendar days in order to identify a suspect. However, in no event may the bank file a suspicious activity report more than sixty days after the date of detection.[15]

[13] 31 C.F.R. § 103.18(a)(2) (31 C.F.R. § 1020.320(a)(2)).
[14] 31 C.F.R. § 103.18(a)(2)(i)-(iii) (31 C.F.R. § 1020.320(a)(2)(i)-(iii)).
[15] 31 C.F.R. § 103.18(b)(3) (31 C.F.R. § 1020.320(b)(3)).

Ocean failed to recognize, address and mitigate the risks associated with Venezuela's parallel foreign exchange market or "permuta,"[16] particularly transactions involving Venezuelan broker/dealers (Casa de Bolsa and Sociedad de Corretage). Risks associated with "permuta" transactions include an inability to readily identify the true originator/beneficiary and source of funds, the use of offshore entities and shell companies to facilitate transactions as well as inherent vulnerabilities relative to money laundering and terrorist financing. Ocean failed to routinely validate documents, companies, clients and broker/dealers involved in "permuta" transactions and adequately integrate these practices into its BSA compliance system and controls.

Ocean violated the suspicious activity reporting requirements of 31 U.S.C. § 5318(g) and 31 C.F.R. § 103.18 (31 C.F.R. § 1020.320) by failing to file hundreds of suspicious activity reports in a timely manner. Ocean received wire transfers from Mexican Casas de Cambio that exhibited patterns commonly associated with potential money laundering and Black Market Peso Exchange ("BMPE"),[17] including the nature of the business, high-risk geographic locations of the originator and/or beneficiary, and transaction activity that lacked any business or apparent lawful purpose or was inconsistent with the normal and expected transactions for actual or similar customers.

The absence of effective internal controls, designated personnel properly trained in sufficient numbers, and independent testing to ensure BSA compliance at Ocean resulted in a number of violations of the requirement to report suspicious transactions in a timely manner.

In 2009, Ocean voluntarily reviewed account activity in six different areas for the period 2002 to 2008. Ocean subsequently filed fifty-two suspicious activity reports, reporting in excess of $259 million in suspicious transactions. Many of the suspicious activity reports filed as a result of the transaction reviews were delinquent. Adequate BSA compliance measures for foreign and domestic retail relationships could have enabled Ocean to detect and report suspicious transactions through these accounts in a timely manner, making the information contained within the reports inherently more valuable and available to law enforcement for the initiation or support of ongoing law enforcement investigations. The resulting delays impaired the usefulness of the suspicious activity reports by not providing law enforcement and regulatory agencies with timely information.

D. Failure to File Currency Transaction Reports

FinCEN has determined that Ocean violated the requirement to report transactions in currency. The BSA and its implementing regulations require banks to report transactions that involve

[16] U.S. Department of State Investment Climate Statement, February 2009.
[17] FinCEN Advisory Issue 12, June 1999.

either "cash in" or "cash out" of more than $10,000 during any one business day.[18] A bank must report transactions in currency through the filing of currency transaction reports by the fifteenth calendar day after the day of the transaction.[19] Banks may exempt certain parties from the cash reporting requirements of the BSA, but only after specific requirements have been met.[20]

In 2007, an internal review conducted by the Bank's BSA Compliance Department revealed instances where – during a four month period that same year – currency transaction reports ("CTRs") were not filed. The Bank subsequently conducted a review and filed twenty-nine CTRs which had not previously been filed, amended twenty-four previously filed CTRs, and discovered fifty-four CTRs which were erroneously generated by the system and reported in error.

Improper reports and delays in filing currency transaction reports impaired the usefulness of the currency transaction reports by not providing law enforcement with more timely and accurate information.

IV. CIVIL MONEY PENALTY

Under the authority of the Bank Secrecy Act and the regulations issued pursuant to that Act,[21] FinCEN has determined that a civil money penalty is due for the violations of the Bank Secrecy Act and the regulations issued pursuant to that Act, as described in this ASSESSMENT.

Based on the seriousness of the violations at issue in this matter, and the financial resources available to Ocean, FinCEN has determined that the appropriate penalty in this matter is $10,900,000.

V. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, Ocean without admitting or denying either the facts or determinations described in Sections III and IV above, except as to jurisdiction in Section II, which is admitted, consents to the assessment of a civil money penalty in the sum of $10,900,000. This penalty assessment is being issued concurrently with the Deferred Prosecution Agreement and accompanying $10,988,136 forfeiture by the United States Government and $10,900,000 civil money penalty by the FDIC and FOFR against Ocean. The penalty assessment of FinCEN shall be deemed satisfied fully by the $10,988,136 payment to the United States Government.

Ocean 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

[18] 31 U.S.C. § 5313 and 31 C.F.R. § 103.22(b) (31 C.F.R. § 1010.311).
[19] 31 C.F.R. § 103.22(a) and 31 C.F.R. § 103.27(a)(1) (31 C.F.R. § 1010.306(a)(1)).
[20] 31 C.F.R. § 103.22(d) (31 C.F.R. § 1020.315(a)).
[21] 31 U.S.C. § 5321 and 31 C.F.R. § 103.57(a)-(h) (31 C.F.R. § 1010.820(a)-(h)).

or any employee, agent, or representative of FinCEN to induce Ocean to enter into the CONSENT, except for those specified in the CONSENT.

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

VI. RELEASE

Ocean understands that execution of the CONSENT, and compliance with the terms of this ASSESSMENT and the CONSENT, constitute a complete settlement and release of civil liability for the violations of the Bank Secrecy Act and regulations issued pursuant to that Act as described in the CONSENT and this ASSESSMENT against the Bank.

By:

/s/

_____

James H. Freis, Jr., Director

FINANCIAL CRIMES ENFORCEMENT NETWORK

U.S. Department of the Treasury

Date: _____