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

IN THE MATTER OF:	)	
	)	
	)	
EUROBANK	)	**Number 2010-2**
SAN JUAN, PUERTO RICO	)	

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 has determined that grounds exist to assess a civil money penalty against Eurobank ("Eurobank" or the "Bank"). Eurobank enters into the CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY ("CONSENT") without admitting or denying the determinations by the Financial Crimes Enforcement Network, 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

Eurobank is a commercial bank with 23 branches located throughout Puerto Rico, which has been designated as both a High Intensity Drug Trafficking Area ("HIDTA") since 1994 and a High Risk Money Laundering and Related Financial Crimes Area ("HIFCA") since 2000. Eurobank is an insured Commonwealth-chartered nonmember bank located in San Juan, Puerto Rico. As of December 31, 2009, the Bank had total assets of approximately $2.56 billion, and posted a net loss of nearly $71 million. The Federal Deposit Insurance Corporation ("FDIC") is Eurobank's Federal functional regulator and examines the Bank for compliance with the BSA and its implementing regulations and with similar rules under Title 12 of the United States Code. The Office of the Commissioner of Financial Institutions ("OCFI") examines Eurobank for compliance with requirements under banking laws of the Commonwealth of Puerto Rico comparable to those of the BSA and its implementing regulations.

---

[1] 31 U.S.C. § 5311 et seq. and 31 C.F.R. Part 103.

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

III. DETERMINATIONS

A. Summary

Eurobank violated the requirement to establish and implement an adequate anti-money laundering program. Breakdowns in the Bank's anti-money laundering program caused the Bank to fail to effectively identify and report transactions that exhibited indicia of money laundering or other suspicious activity, relative to the types of products and services offered by the Bank, the volume of its business, and the nature of its customers. The civil money penalty by the Financial Crimes Enforcement Network is the result of deficiencies and transactions that occurred, in large part, at the Bank between April 2005 and December 2008.

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

The Financial Crimes Enforcement Network has determined that Eurobank violated the requirement to establish and implement a reasonably designed anti-money laundering program. Since April 24, 2002, the BSA and its implementing regulations have required banks to establish and implement anti-money laundering programs.[3] 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.[4] The FDIC requires each bank under its supervision to establish and maintain an anti-money laundering 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.[5]

The Bank failed to implement all four core elements of an adequate anti-money laundering program to ensure compliance with the BSA and manage the risk of money laundering or other suspicious activity.

1. *Internal Controls*

Eurobank failed to implement policies, procedures, and internal controls reasonably designed to comply with the BSA and manage the risk of money laundering. The Bank conducted business without adequate systems and controls, as appropriate and practical, to detect and timely report suspicious activity.

The Bank repeatedly failed to implement effective internal controls to ensure compliance with the BSA between April 2005 and December 2008, with recurring adverse findings

---

[2] 31 U.S.C. § 5312(a)(2) and 31 C.F.R. § 103.11.
[3] 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 103.120.
[4] *Id.*
[5] 12 C.F.R. § 326.8(b) and (c).

identified by its supervisory agencies. During this time period, the Bank failed to implement systems and procedures adequately designed to assess the Bank's overall BSA/anti-money laundering ("BSA/AML") risk, perform customer due diligence, identify high-risk customers, perform commensurate due diligence of customers that were identified as high-risk, and monitor for suspicious activity, resulting in numerous failures to identify and timely report suspicious activity.

Eurobank's overall risk assessment was inadequate. Without appropriate analysis and inquiries, the assessment neither adequately supported assigned risk ratings for services provided by the Bank, nor addressed all areas of the Bank including leasing, wire transfers, pouch activity, the Trust Department, privately-owned automated teller machines, non-customer services such as cashing "on-us" checks, sales of monetary instruments, and merchant credit card processing.

Eurobank's due diligence policies and procedures for assessing customer risk were deficient. Customer profiles were missing altogether, or provided too little information to ascertain a customer's potential risk. Remedial measures for the Bank's due diligence policies and procedures were either not implemented or implemented inadequately, even after the adverse findings and formal action by the Bank's Federal functional regulator. For example, when the Bank revised its due diligence procedures in July 2007, the Bank did not apply the revised procedures to accounts created before July 2007. Sample testing conducted by examiners in October 2007, revealed that over 93 percent of sampled accounts lacked evidence that the Bank conducted adequate customer due diligence. Available account information revealed that in 60 percent of these cases, the required customer due diligence form was incomplete, while the remaining 40 percent did not have any customer due diligence forms.

A pervasive failure to implement adequate procedures to identify high-risk customers over the course of multiple years was evident, and contributed to the Bank's inability to adequately monitor, identify, and report suspicious activity. The Bank's risk rating process was ineffective and was not regularly reassessed to ensure that all high-risk customers were identified. The Bank was unable to identify all of its high-risk customers due to deficiencies in its risk rating methodology, leading to a failure to identify and report suspicious activity in a timely manner. At one point, the Bank only identified a customer as high-risk if the customer had an average balance of $250,000 or more in a checking or savings account, or performed cash transactions totaling over $250,000 a month.

Even after the imposition of the March 15, 2007, Cease and Desist Order by the FDIC, the Bank still had not developed a risk rating system capable of identifying all high-risk accounts in the Bank's existing customer database, or new high-risk accounts at account opening, despite being cited for these deficiencies in previous examinations. The Bank had identified only 331 high-risk customers by December 31, 2007, and still had not assigned a risk rating to 1,528 accounts. Numerous high-risk customers were not on the Bank's high-risk list, and potentially higher-risk customers such as money services businesses, privately-owned automated teller machines, cash-intensive businesses, and professional services providers, as well as services such as monetary instrument sales and wire transfers, were not properly risk-rated. Although management was aware that the Bank's risk rating process was flawed and risk matrix was not tested to determine if all high-risk customers would be identified, it did not correct these

deficiencies before implementing a new automated monitoring system in November 2008, thus rendering the new system ineffective for identifying suspicious activity.

In 2006, as many as 55 high-risk accounts, including cash-intensive businesses, money services businesses, offshore corporations, and a pawn shop were not identified as potentially high-risk. As noted above, the Bank often failed to accurately designate accounts as high-risk, including customers conducting wire transfers to high-risk countries, and cash intensive businesses. Over 87 percent of sampled accounts involving significant international wire activity were not identified as high-risk. More recently, in a High-Risk Account Reconciliation report provided by the Bank in 2009, 93 customers that regularly conducted international wire transfers were not captured by the Bank's risk matrix.

Review of high-risk accounts was inadequate and often not performed within a reasonable period of time. Procedures for conducting commensurate due diligence on high-risk customers were flawed. There were no procedures in place to validate customer risk profiles, explain significant changes in transaction behavior, or place parameters on variances from expected transaction behavior. Instead of assessing activity that varied from expected activity for identifying suspicious transactions, the Bank changed the customer's profile to reflect the actual activity, thereby negating any ability to detect suspicious activity.

Out of 10 high-risk customer files sampled by examiners in 2006, six had outdated financial statements and two had no financial statements. No actual analysis was found in any of the sampled files to support the customers' anticipated account activity, cash needs, or sources of income. Subsequent transaction testing by examiners in 2007 revealed that no commensurate review procedures had been completed for 11 accounts that were regarded by the Bank as high-risk. As of December 2008, commensurate due diligence had not been conducted yet on over 200 high-risk accounts opened prior to and during 2008. The Bank did not review the customer statements and anticipated activity for newly identified high-risk accounts until at least 6 months after the account was opened. Because of the workload associated with assessing the backlog of high-risk accounts, medium and low-risk accounts had not been subject to any periodic review.

Suspicious activity monitoring at the Bank was inadequate between April 2005 and December 2008. As a result, suspicious activity went undetected and unreported or was reported delinquently. The Bank consistently failed to adequately monitor certain significant services for suspicious activity for 3 consecutive years, including wire transfers and monetary instrument sales. The Bank's use of manual processes to monitor for suspicious activity during much of the time period rendered the risk ratings applied by the Bank practically irrelevant. The Bank's use of manual processes for suspicious activity monitoring was particularly inadequate given the Bank's customer base, geographic risk and business lines, as well as the volume, scope, and types of transactions conducted at the Bank. Because the Bank failed to develop appropriate procedures and policies to detect, monitor, and report suspicious activity, no risk tolerance parameters had been established for the monitoring of cash transactions, wire transfers, and monetary instruments. Branch personnel could not readily identify suspicious activity. Documentation supporting the decision not to file a suspicious activity report was absent in several cases, and some suspicious activity report investigations had been open and pending a final resolution for nearly 2 years.

The Bank's use of automated systems to monitor for suspicious activity was continually deficient between April 2005 and December 2008. The suspicious activity monitoring program in use until November 2008 failed to adequately capture numerous services provided by the Bank, including lending, trade financing, pouch activities, and check deposits. The Bank did not monitor for suspicious activity based on customers' risk profiles, or the type and/or volume of customers' transactions. As a result, the Bank relied predominantly on manual processes to monitor for suspicious activity during most of the period under consideration. When the Bank replaced its old monitoring system in favor of a new one in November 2008, it failed to conduct appropriate system validation and parameters testing to ensure that the new system could adequately identify suspicious activity. Procedures established for the new system were neither risk-based nor tailored to the Bank's customer base, geographic risk, or business lines.

2. *Designated Individual or Individuals to Coordinate and Monitor Day-to-Day Compliance*

The Bank's BSA compliance area was not adequately staffed with qualified personnel for over 3 years. Management failed to hire knowledgeable and experienced personnel to fill this critical role despite serious, repeated criticism of the Bank's BSA program. Staffing levels were inadequate for the Bank's size and risk profile. Since March 2007, the Bank has retained three different BSA Officers. The first individual was terminated in February 2008 after presiding over the inadequate implementation of the Bank's BSA/AML program. The second of three BSA Officers possessed limited BSA experience and lacked sufficient staffing to manage day-to-day BSA operations. As a result, the second BSA Officer was replaced by the Bank in 2009.

3. *Training for Appropriate Personnel*

The Bank failed to ensure appropriate personnel were adequately trained on BSA requirements. Over a quarter of employees had not received annual training. Furthermore, the Bank did not ensure that appropriate employees were sufficiently trained to comply with BSA requirements, even after being required to do so under the March 15, 2007, Cease and Desist Order. Training conducted in both 2006 and 2008 was clearly ineffective based on the significant BSA deficiencies discovered between April 2005 and December 2008. Moreover, testing conducted in 2009 found that both branch and BSA personnel were unable to readily identify suspicious activity.

4. *Independent Testing*

The Bank's independent testing function has been deficient since at least 2006. In 2006, adverse internal audit findings had not been discussed with the Compliance Officer or presented to the Board of Directors. The audit report did not identify many of the BSA deficiencies identified by regulatory authorities during the timeframe, and the scope of the audit was not adequate, since it failed to include an overall assessment of the effectiveness of the BSA/AML program. In October 2007, the independent testing program failed to include validation of the Bank's BSA risk assessment and risk matrix. Although the procedures were updated during the October 2007 exam for auditing the BSA risk assessment, it took an inordinate amount of time (6 months) to complete testing of the risk assessment and risk matrix, which in turn delayed the implementation of necessary remedial actions. The Bank's response to independent testing

recommendations for such areas as risk assessment, commensurate due diligence for high-risk customers, and wire transfer activity was inadequate, and longstanding deficiencies, identified over the course of multiple audit cycles, were not corrected. Twenty-three observations made by the Bank's Internal Audit Department relating to the risk rating matrix were either improperly addressed or dismissed by Bank management. Some of the Bank's products and services, related to mortgages, leases and merchant credit card programs were outside the scope of the independent audit for BSA compliance. Also, the Bank's internal audit did not adequately validate the accuracy of the Reportable Currency Transaction report. The scope of the audit was limited to cash transactions conducted in a limited number of demand deposit accounts, without any regard to other customer or non-customer transactions.

C. Violations of the Requirement to Report Suspicious Transactions

The Financial Crimes Enforcement Network has determined that Eurobank violated the suspicious transaction reporting requirements of the BSA and regulations issued pursuant to that Act.[6] These reporting requirements 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.[7] A transaction is suspicious if the transaction: (i) involves funds derived from illegal activities or is conducted in order to hide or disguise funds or assets derived from illegal activities, (ii) is designed to evade reporting or recordkeeping requirements under the BSA (e.g., structuring transactions to avoid currency transaction reporting), or (iii) 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 bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[8]

Banks must report suspicious transactions by filing suspicious activity reports and must generally do so no later than thirty (30) calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing such reports.[9] If no suspect was identified on the date of detection, a bank may delay the filing for an additional thirty (30) calendar days in order to identify a suspect, but in no event may the bank file a suspicious activity report more than sixty (60) calendar days after the date of initial detection.[10]

When filing a suspicious activity report, the financial institution must provide a detailed description of the activity at issue. A description of the transaction or transactions "is critical."[11] The form clearly states that the care with which the description of the activity is written "may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood."[12] If a financial institution fails to file a complete suspicious activity report, the report may not provide adequate information to alert law enforcement to the existence of potentially serious criminal activity.

---

[6] 31 U.S.C. § 5318(g) and 31 C.F.R. § 103.18.
[7] 31 C.F.R. § 103.18(a)(2).
[8] 31 C.F.R. § 103.18(a)(2)(i)-(iii).
[9] 31 C.F.R. § 103.18(b).
[10] 31 C.F.R. § 103.18(b)(3).
[11] *See* Part V: Suspicious Activity Information Explanation/Description, Suspicious Activity Report, TD F 90-22.47.
[12] *Id.*

The absence of an adequate anti-money laundering program resulted in numerous violations of the requirement to timely report suspicious transactions over an extended period of time. The Financial Crimes Enforcement Network determined that Eurobank filed 305 initial suspicious activity reports from 2005 through 2008. Of these, 146 (48 percent), were not timely filed. The average delinquency rate ranged from approximately 23 percent in 2005 to 58 percent in 2007. In 2008, almost a year after the 2007 Cease and Desist Order was imposed by the FDIC, nearly 45 percent of all of Eurobank's initial suspicious activity report filings were not timely filed. The 2007 Cease and Desist Order addressed suspicious activity reporting deficiencies such as inadequate monitoring for suspicious activity across the Bank's business lines, failing to investigate suspicious activity in a timely and complete manner, and failing to file suspicious activity reports in a complete, timely, and accurate manner. The total dollar amount of suspicious activity involved in the delinquent suspicious activity reports was approximately $66 million. The vast majority of suspicious activity reports filed were for suspected structuring and money laundering activity. While the Financial Crimes Enforcement Network understands that certain situations may require time to conduct an appropriate review to determine whether activity is suspicious and for purposes of a complete and accurate report, Eurobank exhibited a pattern of consistently filing delinquent suspicious activity reports for an extended period of time. The resulting delays impaired the usefulness of the suspicious activity reports to law enforcement.

A review of monetary instruments purchased between April and June of 2006 identified 58 customers who performed potentially suspicious transactions that went undetected by the Bank. Of these, 10 customers structured money order and official check purchases. Further review of the accounts determined that the activity involved well over $500,000 in suspicious transactions, and involved a period ranging from as far back as April 2005 through September 2006, before the Bank began filing suspicious activity reports on the activity at the direction of examiners in October 2006. In another example, Eurobank failed to file complete, timely, and accurate suspicious activity reports for at least 10 customers whose suspicious transactions involved over $2.5 million. The suspicious transactions went undetected by the Bank for up to 14 months, and unreported until identified by examiners in December 2008.

IV. CIVIL MONEY PENALTY

Under the authority of the BSA and the regulations issued pursuant to that Act,[13] the Financial Crimes Enforcement Network has determined that a civil money penalty is due for violations of the BSA and the regulations implementing that Act, as described in this ASSESSMENT.

Based on the seriousness of the violations at issue in this matter, and the limited financial resources available to Eurobank, the Financial Crimes Enforcement Network has determined that the appropriate penalty in this matter is $25,000. This penalty shall be concurrent with a $25,000 civil money penalty assessed by the FDIC, and shall be satisfied by one payment of $25,000 to the United States Department of the Treasury.

---

[13] 31 U.S.C. § 5321 and 31 C.F.R. § 103.57.

V. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, Eurobank, 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 $25,000.

Eurobank 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 the Financial Crimes Enforcement Network or any employee, agent, or representative of the Financial Crimes Enforcement Network to induce Eurobank to enter into the CONSENT, except for those specified in the CONSENT.

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

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

By:

/s/

James H. Freis, Jr., Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury

Date: April 22, 2010