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

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2012-01**
First Bank of Delaware	)	
Wilmington, Delaware	)	

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 First Bank of Delaware ("First Bank" or the "Bank"). First Bank 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.

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5314, 5316-5332. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Chapter X (formerly 31 C.F.R. Part 103). On March 1, 2011, a transfer and reorganization of BSA regulations from 31 C.F.R. Part 103 to 31 C.F.R. Chapter X became effective. Throughout this document we refer to Chapter X citations. A cross-reference index of Chapter X and Part 103 is located at http://www.fincen.gov/statutes_regs/ChapterX/.

II. JURISDICTION

First Bank is an insured state-chartered nonmember bank located in Wilmington, Delaware. As of December 31, 2011, the Bank reported a net income of $1.5 million. The Federal Deposit Insurance Corporation ("FDIC") is First Bank'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. At all relevant times, First Bank was a "financial institution" and a "bank" within the meaning of the BSA and the regulations issued pursuant to the Act.[2]

III. DETERMINATIONS

The Financial Crimes Enforcement Network has determined that First Bank violated the Bank Secrecy Act. Since 2008, First Bank willfully (1) lacked an anti-money laundering program reasonably designed to manage risks of potential money laundering and other illicit activity, in violation of Title 31, United States Code, Section 5318(h) and 31 C.F.R. § 1020.210; and (2) failed to detect and adequately report evidence of money laundering and other illicit activity, in violation of Title 31, United States Code, Section 5318(g) and 31 C.F.R. § 1020.320.

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

Since April 24, 2002, the BSA and its implementing regulations have required banks to establish and implement anti-money laundering ("AML") programs.[3] A bank is deemed to have satisfied the requirements of the BSA if it implements and maintains an anti-money laundering

[2] 31 U.S.C. § 5312(a)(2) and 31 C.F.R. §§ 1010.100 and 1020.100.

[3] 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1020.210.

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] As discussed in detail below, First Bank violated the BSA's anti-money laundering program requirements by (1) conducting business without adequate internal controls, (2) failing to conduct adequate independent testing, (3) failing to designate a Bank Secrecy Act Officer to ensure effective day-to-day compliance, and (4) failing to provide training for appropriate personnel.

i. First Bank failed to provide for an effective system of internal controls to ensure ongoing compliance.

First Bank provided consumer and commercial services to a full range of customers, including products and customers that the Bank reasonably should have considered to be high risk for money laundering. Between 2008 and February 2012, the Bank did not effectively assess and implement policies and procedures to mitigate potential money laundering risks, given its high-risk products and clients, and failed to detect and timely report suspicious activity to FinCEN.

[4] 31 C.F.R. § 1020.210.

[5] 12 C.F.R. § 326.8(b) and (c).

Risks Associated with Third-Party Payment Processors.

Third-party payment processors serve as intermediaries between merchants and banks. Financial regulators have long recognized the inherent money laundering risks associated with this industry and specific guidance to banks on the risks associated with third-party payment processors, and systems and controls to manage those risks, has been available since 2008.[6] Despite this guidance, First Bank repeatedly accepted third-party payment processors as customers but failed to adequately assess AML risks associated with these customers. In addition to failing to create and maintain a comprehensive program to manage such AML risks, First Bank also consistently ignored specific red flag indicators associated with their particular customers.

First Bank facilitated consumer fraud and abuse by originating electronic transactions on behalf of dishonest third-party payment processors and merchants by providing them with access to consumer bank and credit card accounts without proper BSA controls. Several third-party payment processor customers had documented histories of Federal Trade Commission Act violations, but there was no evidence that appropriate Bank personnel investigated these "red flags." Moreover, First Bank failed to collect sufficient information to anticipate the normal range of activities and transactions for these customers, which resulted in the Bank failing to take into account heightened risk factors, such as high unauthorized return rates, in monitoring the activities of its automated clearing house ("ACH") merchant customers. As a result, high-risk

---

[6] *See* Office of the Comptroller of the Currency (OCC), *Bulletin OCC-2008-12: Payment Processors,* April 24, 2008; FDIC, *FIL-127-2008: Guidance on Payment Processor Relationships,* November 7, 2008; Federal Financial Institutions Examination Council, *2010 Bank Secrecy Act/Anti-Money Laundering Examination Manual,* pp. 239-241. In addition, after the time period of the conduct alleged in this case, FinCEN issued recent guidance on current risks associated with third-party payment processors. See FinCEN Advisory FIN-2012-A010 (Oct. 22, 2012).

third-party payment processors and merchant customers using their services were not identified or appropriately monitored. Even to the extent that the Bank did have a policy governing such risk, the Bank accepted customers in direct violation of its own written BSA/AML policy.

In addition to systemic failures of its AML/BSA compliance program, First Bank failed to detect and act upon significant risk indicators regarding their customers. For example, First Bank's Remotely Created Check ("RCC") service was created as a major component of its E-Payments business line. First Bank served as the depository institution for five RCC third-party payment processors. From the earliest activity in the RCC service, potential BSA/AML compliance risks were evident, including much higher transaction rates than originally anticipated as the program experienced rapid growth, as well as high rates of unauthorized returns. Merchants utilizing the RCC service were responsible for total return rates of over 60%, which vastly exceeded any reasonably expected rate for such activity. Merchants utilizing the RCC service were responsible for unauthorized return rates of up to 8%, which was over 250 times the average ACH rate for 2010 of 0.03%.[7] Two merchant clients of one RCC service customer had unauthorized return rates of 5% for five and six month periods. Despite this, they were not terminated immediately, which was in contravention of the Bank's own RCC policy. The Bank failed to recognize or adequately investigate this activity as suspicious during the program's existence.

In addition, until November 2011, First Bank served as a depository institution for third-party payment processors servicing merchants paid through the Automated Clearing House Network. Activity and revenue from this business line was significantly higher than anticipated.

---

[7] NACHA – The Electronic Payments Association, *10 Years of the ACH Quality Initiative* (April 4, 2011), p.3.

In 2010, the Bank processed over $1.4 billion in ACH transactions, primarily through a single customer. The Bank failed to collect sufficient information on this customer, as well as the customer's major ACH merchant clients, and failed to adequately assess associated risks.[8] For example, through its primary ACH third-party payment processor customer, the Bank processed almost $22 million in ACH transactions in 2010 for a foreign-based money services business ("MSB") that was in the business of "facilitating banking transactions." First Bank's customer file on the MSB contained minimal information, lacked necessary financial disclosure information, and did not include evidence of address verification, site visits (in contravention of the Bank's own MSB Policy), background checks, consumer complaint searches, and other relevant due diligence information.

Risks Associated with Money Services Businesses.

First Bank failed to adequately assess BSA/AML compliance risks and failed to implement effective policies and procedures to mitigate risks of high-risk MSB customers. The Bank lacked effective policies, procedures, and practices necessary to ensure that it consistently gathered and reviewed sufficient customer documentation to adequately assess risk and the potential for money laundering, based on each customer's business, products, services, and normal range of activities.

First Bank did not effectively perform individual risk assessments of its MSB customers. For instance, the Bank completed an initial risk assessment of its check casher business line in 2009, but subsequently did not undertake necessary risk reviews despite subsequent rapid growth of the business line. BSA/AML risk analyses were not provided to appropriate Bank personnel,

[8] Federal Financial Institutions Examination Council, *2010 Bank Secrecy Act/Anti-Money Laundering Examination Manual*, "Third Party Payments Processors – Overview," pp. 239-240.

negating the effectiveness of the materials. The Bank also failed to perform on-site visits for out-of-state, high-risk MSB customers, several of which were located in High Intensity Drug Trafficking Areas ("HIDTAs") and High Intensity Financial Crimes Areas ("HIFCAs"). The Bank failed to conduct annual on-site visits for a number of other potentially high-risk MSB customers in contravention of its own policy. Although First Bank's BSA/AML policy with respect to MSBs stated that each MSB with a remote deposit capture ("RDC") machine at its location should be visited on an annual basis, check casher customers of the Bank, including those with RDC machines at their locations, were not visited by Bank personnel.

Among its MSB customers, one offered prepaid cards to foreign persons. With respect to this customer, the Bank lacked adequate policies and procedures to ensure compliance with the BSA and to conduct sufficient monitoring for suspicious transactions. The Bank relied on the customer to perform BSA/AML functions related to this product, but in doing so failed to collect adequate information from its customer on the foreign clients. These deficiencies resulted in First Bank being directed by FDIC to:

- update its policies and procedures related to the customer's activities;
- enhance the Bank's risk assessment to include the information on the customer's products, services, and geographic locations;
- perform an independent review of the customer's BSA/AML program; and
- perform a look back review for suspicious activity.

In addition, First Bank processed sales of Iraqi Dinars for an MSB customer based in Connecticut by accepting payment from purchasers of Dinars through the customer's website. Although the Bank's former Chief Operating Officer advised the Board of Directors that the BSA/AML and risk management departments were involved in the oversight of this new product line, subsequent review determined that Iraqi Dinar sales processing was never explicitly

incorporated into the Bank's BSA/AML policies and procedures. Moreover, had the Bank's customer involved in Iraq Dinar sales been subject to the Bank's MSB Policy, it should have been the subject of a site visit, but the customer was not visited by Bank personnel.

Transaction Monitoring.

First Bank failed to implement and maintain transaction monitoring systems necessary to effectively monitor customer transactions. In light of its deficient customer documentation and across-the-board risk ratings, the Bank ran the risk of failing to effectively monitor its customers' transactions to determine if the actual activity was commensurate with expected activity and/or lacked any apparent business or legal purpose. First Bank's transaction monitoring practices put the Bank at risk of failing to comply with BSA suspicious activity reporting requirements. The Bank's software system merely identified customer deviations from a peer group average and did not compare a customer's actual ongoing activity to the customer's transaction history for inexplicable deviations or spikes. The detection system did not allow for report analysis by name, address, or phone number fields. The Bank's automated system allowed for stratification and evaluation of customer risk ratings, but these functions were not adequately utilized.

ii. **First Bank failed to conduct adequate independent testing for compliance.**

First Bank's independent BSA testing function did not capture and assess risk emanating from its entry into non-traditional banking products, services, and business lines. As a result, comprehensive BSA testing of these products, services, and business lines was not conducted. The scope of the Bank's BSA audit failed to recognize and respond to risk associated with the Bank's elevated risk profile, including increasingly complex and voluminous transaction activity.

iii. **First Bank failed to designate a Bank Secrecy Act Officer to ensure effective day-to-day compliance.**

From at least 2008 through May 2011, the Bank's BSA compliance officer failed to effectively provide day-to-day management of the Bank's BSA/AML compliance program, in light of the Bank's risk profile and volume of activities. The Bank's Board and other appropriate Bank personnel were not notified of numerous instances of potential suspicious activity related to the Bank's third-party payment processing and MSB programs. The BSA Officer failed to escalate BSA problems to senior management. For instance, the BSA Officer was aware of limitations related to the Bank's automated BSA/AML compliance software, but did not appropriately address this deficiency.

iv. First Bank failed to adequately provide training for appropriate personnel.

The Bank failed to ensure appropriate personnel were adequately trained on BSA requirements. The Bank did not develop and implement a BSA/AML training program for appropriate personnel commensurate with First Bank's risk profile. The Bank's computer-based BSA training did not adequately address the risk associated with the Bank's non-traditional business lines, including the RCC, MA, ACH, and MSB products and services. The absence of training appropriate to the Bank's overall heightened risk profile made the Bank vulnerable to facilitating the movement of illicit proceeds and noncompliance with the BSA.

B. Violations of the Requirement to Report Suspicious Transactions

The Financial Crimes Enforcement Network has determined that First Bank violated the suspicious transaction reporting requirements of the BSA and its implementing regulations.[9] 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

[9] 31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320.

"knows, suspects, or has reason to suspect" are suspicious.[10] 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 record keeping 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.[11]

The absence of an effective anti-money laundering program at First Bank resulted in numerous violations of BSA suspicious activity reporting requirements over an extended period of time. Weak internal controls led to an egregious failure of First Bank's ability to effectively detect and report suspicious activity. Bank management failed to implement effective policies and procedures to ensure that suspicious activity associated with third-party payment processors and the Bank's high-risk MSB customers was consistently identified and reported. The Bank failed to adequately investigate high return rates and excessive unauthorized return rates and other red flags, despite requirements in the Bank's written policy. As a result, suspicious activity went undetected and unreported in violation of the BSA. For example, the Bank failed to adequately detect and report suspicious activity related to a customer doing business as a shopping club, with a return rate over 32% and an extensive, publicly available complaint history. The customer accounted for over $64 million in ACH transactions during 2010.

[10] 31 C.F.R. § 1020.320(a)(2).

[11] 31 C.F.R. § 1020.320(a)(2)(i)-(iii).

The Financial Crimes Enforcement Network determined that First Bank has filed approximately 150 suspicious activity reports since 2007 involving subjects not previously reported by the Bank. Of these reports, approximately 46, or nearly a third, were late and involved over $1.6 billion in suspicious activity. In nearly every late report, a year or more elapsed from the time of the underlying suspicious activity to the preparation of the suspicious activity report by First Bank. In several cases, the delay was significantly longer than a year before the initial report was prepared by the Bank. On two separate occasions, the Bank was directed by FDIC to perform look back reviews to identify suspicious activity related to products and services offered by the Bank over which the Bank had inadequate BSA/AML oversight to ensure compliance. In one instance, a report should have been filed in December 2008, but was not filed until February 2012. First Bank exhibited a pattern of consistently filing late suspicious activity reports for an extended period of time. The resulting delays impaired the usefulness of the suspicious activity reports to law enforcement.

IV. CIVIL MONEY PENALTY

Under the authority of the Bank Secrecy Act and the regulations issued pursuant to that Act,[12] the Financial Crimes Enforcement Network has determined that a civil money penalty is due for violations of the Bank Secrecy Act 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 financial resources available to First Bank, the Financial Crimes Enforcement Network has determined that the appropriate penalty in this matter is $15,000,000. This penalty shall be concurrent with a

[12] 31 U.S.C. § 5321 and 31 C.F.R. § 1010.820.

$15,000,000 civil money penalty assessed by the Office of the United States Attorney for the Eastern District of Pennsylvania, and a $15,000,000 civil money penalty assessed by the FDIC, and shall be satisfied by one payment of $15,000,000 to the United States Department of the Treasury.

V. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, First Bank, 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 $15,000,000.

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

First Bank 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. First Bank 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

First Bank 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 Bank Secrecy Act and regulations issued pursuant to that Act as described in the CONSENT and this ASSESSMENT.

By: /S/ 11/13/12

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