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

IN THE MATTER OF:	)	
	)	
	)	**Number 2010 - 1**
WACHOVIA BANK,	)	
NATIONAL ASSOCIATION	)	
CHARLOTTE, NORTH CAROLINA	)	

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 Wachovia Bank, National Association, Charlotte, North Carolina ("Wachovia" or "the Bank"). Wachovia 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

Wachovia is a nationally chartered bank and subsidiary of Wells Fargo & Company ("Wells Fargo"), a financial institution holding company headquartered in San Francisco, California. The holding company merger of Wachovia Corporation and Wells Fargo & Company was consummated on December 31, 2008. The bank merger transaction in which Wachovia will merge with and into Wells Fargo Bank, N.A., Sioux Falls, South Dakota ("Wells Fargo Bank") may occur on March 20, 2010. Wachovia has over 3,000 locations throughout the United States. Wachovia provides a wide range of financial services to consumers, small

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

businesses, middle-market companies and major corporations. The Office of the Comptroller of the Currency ("OCC") is the Bank's Federal functional regulator and examines Wachovia for compliance with the BSA, its implementing regulations and similar rules under Title 12 of the United States Code.

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

FinCEN may impose civil money penalties, or take additional enforcement action, against a financial institution for violations of the BSA and the regulations issued pursuant to that Act.[3]

III. DETERMINATIONS

A. Summary

An investigation recently conducted by the Internal Revenue Service, the Drug Enforcement Administration and FinCEN, working in conjunction with the United States Attorney's Office for the Southern District of Florida, and a parallel examination and investigation conducted by the OCC, determined that from 2004 to 2008, Wachovia violated the anti-money laundering program requirements, suspicious activity reporting requirements, and Section 312 of the USA PATRIOT Act.[4] Appearing below is a summary of the violations of the BSA by Wachovia.

The anti-money laundering ("AML") program at Wachovia 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. Namely, the Bank failed to:

- establish and implement effective internal policies, procedures, and 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.

Wachovia 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. Wachovia failed to implement a program commensurate with the risks inherent within its business lines and geographical reach. As a result, Wachovia failed to timely file thousands of suspicious activity and currency transaction

---

[2] 31 U.S.C. § 5312(a)(2) and 31 C.F.R. § 103.11.
[3] 31 U.S.C. § 5321 and 31 C.F.R. § 103.57.
[4] 31 U.S.C. § 5318(h)(1), 31 C.F.R. § 103.120, 31 C.F.R. § 103.176 and 31 C.F.R. § 103.18.

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

FinCEN has determined that Wachovia 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] The BSA also requires that an AML program contain the following elements: (1) a system of internal controls; (2) independent testing for compliance; (3) the designation of an individual, or individuals, to coordinate and monitor day-to-day compliance; and (4) training of appropriate personnel.[6]

1. Internal Policies, Procedures and Controls

Wachovia failed to implement an effective system of internal controls to ensure compliance with the BSA and manage the risks of money laundering primarily in its international correspondent banking customers' accounts. Wachovia lacked adequate written policies, procedures and controls reasonably designed to assess the risks of money laundering and ensure the detection and reporting of suspicious transactions.

Wachovia's policies, procedures and controls failed to ensure that the Bank gathered and reviewed sufficient information on foreign correspondent account customers to adequately assess risk and potential for money laundering. A sampling of foreign correspondent customer files showed significant gaps and inaccuracies 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. Documentation of customer identification was not subject to adequate quality controls to ensure the accuracy of information. Furthermore, the Bank lacked an adequate system for periodically updating customer information. The authority to establish or amend expected activity profiles was not clearly defined and failed to require approval of the BSA officer or senior management.

The Bank's enhanced due diligence files were not readily available to key compliance officials. The Bank also failed to update or conduct periodic reviews of foreign correspondent 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.

---

[5] 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 103.120.
[6] Id.

Wachovia also failed to implement an adequate risk-rating methodology that evaluated correspondent 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 foreign money transmitters as "high risk" or "very high risk," it did not apply commensurate enhanced due diligence practices and transaction monitoring methodologies to manage recognized risk. These deficiencies impaired the Bank's ability to appropriately assess the risks associated with particular customers.

Wachovia lacked adequate systems and controls to monitor transactions conducted by its international correspondent bank customers for potential money laundering or other suspicious activity. Wachovia's automated transaction monitoring systems were inadequate to support the volume, scope, and nature of international money transfer transactions conducted by the Bank. The automated transaction monitoring systems were designed to monitor international correspondent transactions at the bank level, and were not designed to readily identify suspicious elements, "Red Flags" or suspicious activity associated with individual transactions. In addition, the monitoring system's programming, methodology, and effectiveness were not independently validated to ensure that the models were detecting potentially suspicious activity.[7]

The number of alerts or events generated by the Bank's automated transaction systems was capped to accommodate the number of available compliance personnel. Each alert or event on an international correspondent bank generated by the Bank's automated transaction monitoring system was comprised of as many as 30,000 individual transactions (with an average of 1,400 transactions per alert), which rendered the monitoring system practically unmanageable. The monitoring system was routinely tuned so that the number of alerts generated by the system with respect to international correspondent banks remained constant at around 300 each month. As a result, the Bank instituted arbitrary limits on the flagging and review of transactions for suspicious activity based solely on the inadequate number of staff available to review these alerts. There is little record of the Bank ever having conducted analysis to determine whether its number of monthly alerts was appropriate to actual risk and the number and nature of transactions facilitated. Despite the fact that Wachovia conducted in excess of six million wire transfers for international correspondent bank customers per month, at times the monitoring system dedicated to international correspondent bank wire transactions, which supplemented the system that reviewed all customer account activity, generated as few as 80 alerts per month. Evidence suggests that as late as September of 2008, as few as 120 wire alerts were generated by the Bank's transaction monitoring system relative to its international correspondent bank customers. Once the caps were removed from the Bank's transaction monitoring system in April

[7] BSA/AML Examination Manual, page 64, 8/24/07.

of 2009, the system began to generate a fluctuating amount of alerts (at times in excess of 500) with respect to international correspondent bank wire transactions.

A review of alerts from the primary automated monitoring system used by Wachovia from August 1, 2007 to August 31, 2008, determined that a majority of foreign correspondent bank accounts did not generate alerts and were not subjected to detailed transaction review despite the high-risk business profiles and geographies associated with many of the customers.

Management failed to document or explain filtering criteria, thresholds, and how both were appropriate for the Bank's risks. Management failed to periodically review and update the filtering criteria and thresholds established for continued effectiveness.

The Bank placed greater emphasis on clearing alerts and eliminating backlogs than reviewing and reporting possible suspicious activity. In 2008, a unit within the Bank reviewed and cleared a backlog of approximately 5,000 cash alerts generated by the Bank's Large Currency Transaction Retrieval System. These alerts were not referred for further review to determine whether possible suspicious activity needed to be reported, and instead were closed following the filing of a currency transaction report. The 2008 review of these 5,000 cash alerts determined that 30% involved round dollar transactions, transactions greater than or equal to $9,000, or consecutive day transactions. A further review of 100 sample alerts determined that 85% exhibited indicia of suspicious activity and should have been referred for further evaluation. In addition, the Bank had a practice of clearing cash alerts based solely on a single instance of structuring. It was not until the spring of 2008 that the Bank curtailed this practice.

a. Failure to Manage Risk of Remote Deposit Capture

Wachovia utilized Remote Deposit Capture ("RDC") to process certain deposit items from its non-United States correspondent accounts. RDC, a deposit transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations such as financial institution branches, ATMs, domestic and foreign correspondents, or locations owned or controlled by commercial or retail customers of the financial institution. In substance, RDC is similar to traditional deposit delivery systems at financial institutions such as pouch activities. However, RDC enables customers of financial institutions to deposit items electronically from locations globally. RDC introduces additional risks beyond traditional deposit delivery systems.

Prior to and after the implementation of RDC in May of 2005, the Bank failed to identify and assess certain compliance and operational risks associated with the new system. The Bank did not implement the computer coding necessary to include items deposited through RDC in its supplemental AML monitoring of check activity. As a result, the Bank failed to detect, review and report large volumes of large denomination sequentially numbered traveler's checks

processed through RDC for its non-United States customers' correspondent accounts. During a two-year period, the Bank failed to adequately monitor approximately six million checks valued at nearly $47 billion received through RDC. The Bank discovered this lapse in November of 2007 during an internal investigation involving more than one billion dollars in sequentially numbered commercial checks, received over a two-year period, from a single customer of one of its non-United States correspondent accounts. Once discovered, the Bank filed numerous delinquent suspicious activity reports involving the receipt of tens of millions of dollars in sequentially numbered traveler's and commercial checks by way of RDC from its non-United States correspondent customer accounts.

The Bank failed to adequately incorporate policies and procedures and implement systems and internal controls to manage all of the AML risks associated with RDC. The Bank failed to allocate adequate compliance resources, and should have performed periodic reviews and generated risk management reports on the AML monitoring issues associated with the implementation and ongoing operation of RDC systems and services. The institution failed to consider whether, and to what extent, it could be exposed to the risk of money laundering and non-compliance with AML laws and regulations. In particular, the Bank failed to recognize and respond to the growing use and accompanying risk of RDC by foreign correspondent financial institutions and foreign money services businesses. Enhanced due diligence and commensurate systems and controls for foreign correspondent accounts are necessary if the RDC capture device emanates from higher risk foreign jurisdictions, or when a customer is otherwise identified as high risk.[8]

b. Failure to Monitor Pouch and Cash Letter Activity

The Bank failed to adequately monitor pouch and cash letter activity for receipt of large denomination $1,000 sequentially numbered monetary instruments and commercial checks from its foreign correspondent customer accounts. A 2006 FinCEN Advisory specifically addressed the deposits of sequentially numbered monetary instruments at U.S. financial institutions by non-bank exchange houses known throughout Latin America as "casas de cambio."[9] The Bank failed to adequately respond to several warnings, beginning in December of 2006, relative to the receipt of large volumes of sequentially numbered traveler's checks in pouches from Mexico. The Bank failed to recognize the risks associated with pouches and cash letters received from jurisdictions with lax or deficient AML structures.

The Bank failed to file timely suspicious activity reports with respect to the receipt of tens of millions of dollars in sequentially numbered $1,000 traveler's checks received from its foreign correspondent bank customers. On those occasions where the Bank filed suspicious

[8] See USA PATRIOT Act § 312, 31 C.F.R § 103.176.
[9] FinCEN Advisory FIN-2006-A003, April 28, 2006.

activity reports, few were filed within the same year of receipt of such instruments. In 2006, the Bank filed a total of four suspicious activity reports related to cash letter activity occurring within the same calendar year. The majority of suspicious activity reports filed by the Bank report activity a year after receipt of such items. A number of these reports were filed as many as three years after receipt of such items. The resulting delays and incomplete information impaired the usefulness of the suspicious activity reports by not providing law enforcement and regulators with more timely and comprehensive information related to the tens of millions of dollars in potentially suspicious transactions.

c. Failure to Monitor Bulk Cash Deposits

Foreign financial institutions maintain accounts at U.S. banks to access the United States financial system and acquire services and products that may not be available in the host jurisdiction. During the period from 2004 to 2007, Wachovia repatriated approximately $10 billion in bulk cash from Mexico into the United States. Internal discussions at the Bank demonstrated that employees of the Bank were aware of the 2006 FinCEN Advisory with respect to bulk cash repatriation.[10] However, the Bank failed to implement adequate procedures and controls to ensure that bulk U.S. dollar deposits received from foreign correspondent customers were monitored for suspicious activity. Furthermore, on those occasions where employees of the Bank identified anomalies in the volume or mix of bulk cash deposits that should have warranted further review, these anomalies were not brought to the attention of the Bank's Compliance or AML Investigative Services groups. Audits and reviews of bulk U.S. dollar cash deposits by the line of business appeared related largely to discussions of profitability and logistics, without regard to BSA compliance or the risks of money laundering.

During the period from 2004 to 2008, only one suspicious activity report was filed by the Bank relative to the receipt of bulk United States dollars from its foreign correspondent customers. The Bank exited the international bulk cash business in 2008.

2. Correspondent Accounts for Non-United States Persons

As amended by Section 312 of the USA PATRIOT Act, the BSA requires that:

Each financial institution that establishes, maintains, administers, or manages a private banking account or a correspondent account in the United States for a non-United States person, including a foreign individual visiting the United States, or a representative of a non-United States person shall establish appropriate, specific, and where necessary, enhanced, due diligence

[10] FinCEN Advisory FIN-2006-A003, April 28, 2006.

policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through these accounts.[11]

One of the central goals of the USA PATRIOT Act was to protect access to the United States financial system by requiring due diligence programs for foreign correspondent accounts. Foreign correspondent accounts, as noted in past United States Senate investigative reports, are a gateway into the United States financial system.[12]

Section 312 of the USA PATRIOT Act added subsection (i) to 31 U.S.C. § 5318 of the BSA. This subsection requires each U.S. financial institution that establishes, maintains, administers, or manages a correspondent account in the United States for a foreign financial institution to take certain AML measures for such accounts. In addition, Section 312 of the USA PATRIOT Act specifies additional standards for correspondent accounts maintained for certain foreign banks.

On January 4, 2006, FinCEN published an interim final rule implementing the due diligence provisions of 31 U.S.C. § 5318(i)(1).[13] Subsequently, on August 9, 2007, FinCEN finalized the regulation, and in doing so implemented the enhanced due diligence provisions with respect to correspondent accounts established or maintained for certain foreign banks.[14]

The term "foreign financial institution" includes:

- A foreign bank;
- Any foreign branch or office located outside the United States of any U.S. broker/dealer in securities, futures commission merchant or introducing broker, or mutual fund;
- Any other person organized under foreign law that, if located in the United States, would be a broker/dealer in securities, futures commission merchant or introducing broker, or mutual fund;
- Any person organized under foreign law that is engaged in the business of, and is readily identifiable as, a currency dealer or exchanger or a money transmitter.[15]

Banks are required to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the bank to detect and report, on an ongoing basis, any known or suspected

---

[11] 31 U.S.C. § 5318(i)(1).

[12] *Correspondent Banking: A Gateway for Money Laundering. See* Senate Hearing 107-84. The report appears on p. 273 of volume 1 of the hearing records entitled *Role of U.S. Correspondent Banking in International Money Laundering*, held on March 1, 2, and 6, 2001.

[13] 31 C.F.R. § 103.176.

[14] 31 C.F.R. § 103.176(b).

[15] 31 C.F.R. § 103.175(h).

money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by the bank in the United States for a foreign financial institution ("foreign correspondent account").[16]

A bank's general due diligence program must include policies, procedures, and processes to assess the risks posed by the bank's foreign financial institution customers. A bank's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. A bank's due diligence program should provide for the risk assessment of foreign correspondent accounts considering all relevant factors, including, as appropriate:

- The nature of the foreign financial institution's business and the markets it serves.
- The type, purpose, and anticipated activity of the foreign correspondent account.
- The nature and duration of the bank's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution).
- The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
- Information known or reasonably available to the bank about the foreign financial institution's AML record,[17] including public information in standard industry guides, periodicals, and major publications.

Wachovia failed to establish appropriate, specific enhanced due diligence policies, procedures and controls reasonably designed to detect and report instances of money laundering through its correspondent accounts for non-United States persons. The deficiencies in the Bank's customer information and risk-rating procedures prevented the Bank from focusing resources on correspondent accounts that posed a high risk of money laundering.[18]

Wachovia maintained correspondent accounts for high-risk casas de cambio in Mexico readily identifiable as engaged in the business of currency dealing, currency exchange and money transmission. The casas de cambio's customers included Mexican centros cambiarios,

---

[16] 31 C.F.R. § 103.176(a); FFIEC BSA/AML Examination Manual, page 109, 8/24/07.

[17] 31 C.F.R. § 103.176(a).

[18] Guidance issued with the interim final rule implementing Section 312 stated that compliance with the due diligence requirements with respect to correspondent accounts for non-U.S. persons would be reasonable if "... it focuses compliance efforts on the correspondent accounts that pose a high risk of money laundering based on an overall assessment of the money laundering risks posed by the foreign correspondent institution. It is the expectation of Treasury that a bank will accord priority to conducting due diligence on high-risk foreign banks for which it maintains correspondent deposit accounts or their equivalents, and will focus foremost on correspondent accounts used to provide services to third parties. Treasury also expects banks to give priority to conducting due diligence on high-risk correspondent accounts maintained for foreign institutions other than foreign banks, such as money transmitters." Anti-Money Laundering Programs; Special Due Diligence Programs for Certain Foreign Accounts, 67 FR 48348, 48350 (July 23, 2002).

dollar exchangers and money remitters. These entities in effect "nested" within the Mexican casa de cambio accounts and Wachovia did not conduct commensurate due diligence and transaction monitoring on those accounts. "Nested" accounts occur when a foreign financial institution gains access to the United States financial system by operating through a United States correspondent account belonging to another foreign financial institution. If the United States bank is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the United States financial system.[19]

Evidence indicative of "nested" accounts within the Mexican casa de cambio accounts was readily discernible within the Bank's own customer files. Despite such evidence, the Bank failed to detect and review these "nested" accounts for suspicious transactions.

In summary, Wachovia failed to implement adequate policies, procedures, systems and internal controls reasonably designed to detect and report instances of money laundering involving at least 13 of its non-bank correspondent accounts. Such measures would have enabled Wachovia to obtain due diligence information on customers of the foreign non-bank entity, as available, and determine whether related transactions conducted in the United States were commensurate with the customers' normal range or expected range of conduct, or lacked any apparent business or lawful purpose.

3. Designation of Compliance Personnel

Wachovia failed to adequately staff the BSA compliance function at the Bank, with individuals responsible for coordinating and monitoring day-to-day compliance with the BSA. The AML Investigative Services unit responsible for monitoring the Bank's correspondent relationships with foreign financial institutions was understaffed, and personnel lacked the requisite knowledge and expertise to adequately perform their duties. At its inception in 2005, the Bank staffed this monitoring unit with as few as three individuals. The Bank failed to recognize the risks inherent within its international business line and provide adequate staffing to mitigate such risks. The Bank's failure to provide adequate designated personnel and training limited its ability to initiate and complete investigations and file complete, accurate, and timely suspicious activity reports.

4. Independent Testing for Compliance

FinCEN has determined that Wachovia's program for independent testing was not effective and failed to ensure compliance with the requirements of the BSA. In view of the inherent risk, the Bank did not implement an effective independent audit function, in terms of

[19] FFIEC BSA/AML Examination Manual, page 171, 8/24/07.

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 Wachovia's suspicious activity monitoring and reporting systems, the Bank's foreign correspondent customer due diligence program, or other aspects of its AML program. Specifically, internal audit did not adequately evaluate and test bulk cash, cash letter, RDC, pouch activities, and the enhanced due diligence process relative to foreign correspondent financial institution accounts.

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. The Bank also suffered from an apparent lack of effective communication between audit, compliance, and management. On the occasions where issues were raised to management, the Internal Audit Department failed to follow up to determine if the Bank had implemented corrective action necessary to address problems raised. Management repeatedly failed to adequately respond to adverse findings and follow the recommendations of both internal and external auditors relative to its foreign correspondent relationships.

C. Violations of the Requirement to Report Suspicious Activity

FinCEN has determined that Wachovia violated the suspicious transactions reporting requirements of the Bank Secrecy Act 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.[20] 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.[21]

Financial institutions must report suspicious transactions by filing suspicious activity reports, generally no later than 30 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 30 calendar days in order to identify a suspect. However,

[20] 31 C.F.R. § 103.18(a)(2).
[21] 31 C.F.R. § 103.18(a)(2)(i)-(iii).

in no event may the bank file a suspicious activity report more than 60 days after the date of detection.[22]

The absence of effective internal policies, procedures and controls, enhanced due diligence relative to foreign correspondent accounts, designated compliance personnel, and independent testing for compliance at Wachovia resulted in numerous violations of the requirement to timely report suspicious activity, as required by the BSA.

Wachovia violated the suspicious activity reporting requirements of 31 U.S.C. § 5318(g) and 31 C.F.R. § 103.18 by failing to file thousands of suspicious activity reports in a timely manner. Wachovia processed over 2.1 million wire transactions totaling nearly $374 billion from May 1, 2004 to May 31, 2007 on behalf of 13 Mexican casa de cambio foreign correspondent customers, most involving parties in the United States and Mexico. Wachovia processed funds transfers for originators and beneficiaries that exhibited patterns commonly associated with potential money laundering, 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 Wachovia resulted in numerous violations of the requirement to report suspicious transactions in a timely manner.

Wachovia conducted a voluntary transaction review, or "Lookback," on the activity of 13 Mexican casa de cambio customers from July 2004 through May 2007. Wachovia filed over 4,200 suspicious activity reports, reporting in excess of $8 billion in potentially suspicious transactions, which represents approximately 17% of the 24,485 suspicious activity reports filed by Wachovia from July 2004 through June 2007. Many of the suspicious activity reports filed as a result of the "Lookback" were delinquent. Adequate BSA compliance measures for non-United States correspondent relationships could have enabled Wachovia 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 and bank regulators 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.

Wachovia failed to file suspicious activity reports subsequent to the receipt of tens of millions of dollars in sequentially numbered $1,000 traveler's checks. The majority of

[22] 31 C.F.R. § 103.18(b)(3).

suspicious activity reports were filed by the Bank a year after receipt of the traveler's checks. A number of such reports were filed three years after receipt of such instruments.

The resulting delays and incomplete information impaired the usefulness of the suspicious activity reports by not providing law enforcement with more timely and concise information related to the hundreds of millions of dollars in suspicious transactions.

Additionally, the Bank failed to recognize the importance of law enforcement inquiries and requests. Such inquiries may include 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.[23] Criminal or grand jury subpoenas with any indicia of money laundering and/or specified unlawful activity may lead to the reporting of suspicious activity which has value to law enforcement authorities outside of the subpoena process. The Bank failed to review, in a timely fashion, a backlog of over 6,700 subpoenas for potential impact upon the suspicious activity reporting process.

D. Failure to File Currency Transaction Reports

FinCEN has determined that Wachovia violated the requirement to report transactions in currency. The Bank Secrecy Act and its implementing regulations require banks to report transactions that involve either "cash in" or "cash out" of more than $10,000 during any one business day.[24] A bank must report transactions in currency through the filing of currency transaction reports and by the fifteenth calendar day after the day of the transaction.[25] Banks may exempt certain parties from the cash reporting requirements of the Bank Secrecy Act, but only after specific requirements have been met.[26]

An internal investigation conducted by Wachovia beginning in 2004, the results of which were disclosed to FinCEN, concluded that the Bank mistakenly continued to exempt 1,624 customers involving at least 3,919 accounts from currency transaction reporting requirements after the merger with First Union National Bank in September of 2001. The improper exemptions were initially granted by First Union National Bank. However, poor management oversight and operating procedures over the integration of currency reporting systems after the merger, including annual reviews in accordance with 31 CFR § 103.22(d)(4), resulted in thousands of violations of 31 CFR § 103.22(b)(1). The continuance of improper exemptions and

---

[23] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, pages 42 – 44.
[24] 31 U.S.C. § 5313 and 31 C.F.R. § 103.22(b).
[25] 31 C.F.R. § 103.22(a) and 31 C.F.R. § 103.27(a)(1).
[26] 31 C.F.R. § 103.22(d).

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

On May 26, 2009, the Bank batch filed the last of 11,053 delinquent currency transaction reports for 118 customers previously and mistakenly exempted.

IV. CIVIL MONEY PENALTY

As noted in Section II above, FinCEN may impose civil money penalties against a financial institution for violations of the Bank Secrecy Act and the regulations implementing that Act.[27] 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 and described in this ASSESSMENT.

After considering the seriousness of the violations and the financial resources available to Wachovia, FinCEN has determined that the appropriate penalty in this matter is $110 million.

V. CONSENT TO ASSESSMENT

To resolve this matter, and only for that purpose, Wachovia 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 $110 million. This assessment is being issued concurrently with the Deferred Prosecution Agreement and accompanying $110 million forfeiture to the United States Government and $50 million civil money penalty by the Office of the Comptroller of the Currency against Wachovia. The penalty assessment of FinCEN shall be deemed satisfied fully by the $110 million forfeiture to the United States Government.

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

Wachovia understands and agrees that the CONSENT embodies the entire agreement between Wachovia and FinCEN relating to this enforcement matter only, as described in Section III above. Wachovia further understands and agrees that there are no express or implied promises, representations, or agreements between Wachovia and FinCEN other than those expressly set forth or referred to in the CONSENT or in this ASSESSMENT. Neither the CONSENT nor this ASSESSMENT are binding on any other agency of government, whether Federal, State, or local.

---

[27] 31 U.S.C. § 5321 and 31 C.F.R. § 103.57.

VI. RELEASE

Wachovia 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: March 12, 2010