Exhibit A

Factual Statement

1. WACHOVIA BANK, N.A. ("Wachovia") is a federally chartered banking institution and subsidiary of Wells Fargo & Company ("Wells Fargo"). Wells Fargo is a publicly-traded financial services company. The Department of the Treasury, Office of the Comptroller of the Currency ("OCC") is Wachovia's primary regulator.

2. Congress enacted the Bank Secrecy Act, Title 31, United States Code, Sections 5311 *et seq.* ("BSA"), and its implementing regulations to address an increase in criminal money laundering activities utilizing financial institutions. Among other provisions, it requires domestic banks, insured banks, and other financial institutions to maintain programs designed to detect and report suspicious activity that might be indicative of money laundering, terrorist financing, and other financial crimes, and to maintain certain records and file reports related thereto that are especially useful in criminal, tax, or regulatory investigations or proceedings.

3. Pursuant to Title 31, United States Code, Section 5318(h)(1) and 12 C.F.R. § 21.21, Wachovia was required to establish and maintain an anti-money laundering ("AML") compliance program that, at a minimum: (a) provides internal policies, procedures, and controls designed to guard against money laundering; (b) provides for an individual or individuals to coordinate and monitor day-to-day compliance with the BSA and AML requirements; (c) provides for an ongoing employee training program; and (d) provides for independent testing for compliance conducted by bank personnel or an outside party.

4. Pursuant to 31 U.S.C. § 5318(i)(1), Wachovia was also required to implement risk-based programs to verify and record the identity of customers opening accounts so that the bank could form a reasonable belief that it knows the true identities of its customers. Each bank's Customer Identification Program ("CIP") must take into account the risks present in various types of accounts, the various kinds of account opening procedures, the various types of identifying information available, and the bank's size, location, and customer base.

5. In particular, pursuant to 31 U.S.C. § 5318(i)(1), banks that manage private banking or correspondent accounts in the United States for non-U.S. persons must establish due diligence, and in some cases enhanced due diligence, policies, procedures, and controls that are designed to detect and report suspicious activity related to certain specified accounts. For foreign correspondent accounts, the Department of Treasury's Financial Crimes Enforcement Network's ("FinCEN") implementing regulations require that the due diligence required under 31 U.S.C.§ 5318(i)(1) include an assessment of the money laundering risk presented by the account based on all the relevant factors including, as appropriate: (i) the nature of the

foreign financial institution's business and the market it serves; (ii) the type, purpose, and anticipated activity of the account; (iii) the nature and duration of the bank's relationship with the account holder; (iv) the anti-money laundering and supervisory regime of the jurisdiction issuing the license for the account holder; and (v) information reasonably available about the account holder's anti-money laundering record.

6. Wachovia was also required, pursuant to 31 U.S.C. § 5318(g), 31 C.F.R. § 103.18, and 12 C.F.R. § 21.11, to file with the Department of the Treasury a Suspicious Activity Report ("SAR"), in accordance with the form's instructions, when it detected the type of activity described below. The requirement became effective on April 1, 1996. According to the form's instructions, Wachovia was required to file a SAR with FinCEN for any transaction conducted or attempted by, at, or through the bank, if it involved or aggregated at least $5,000 in funds or other assets, and the bank knew, suspected, or had reason to suspect that:

> (i) The transaction involved funds derived from illegal activities or was intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation.
>
> (ii) The transaction was designed to evade any requirements promulgated under the Bank Secrecy Act.
>
> (iii) The transaction had no business or apparent lawful purpose or was not the sort in which the particular customer would normally be expected to engage, and the bank knew of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Southern District of Florida Investigation

The Early Investigation

7. Beginning in June 2005, the United States Attorney's Office for the Southern District of Florida, the Drug Enforcement Administration ("DEA"), and the Internal Revenue Service-Criminal Investigation Division ("IRS") began investigating certain wire transfers that were sent to the United States from Mexico. The wired funds were being used for the purchase of aircraft in the United States. Those aircraft were then being used to move illegal narcotics from narcotics-producing countries for ultimate distribution in the United States.

8. The wire transfers were traced back to correspondent bank accounts held by certain Mexican currency exchange houses (commonly referred to as "casas de cambio" or "CDCs") at Wachovia in the United States. The CDC correspondent bank accounts were supervised and

managed by a business unit of Wachovia that was located in Wachovia's offices in Miami, Florida.

9. On numerous occasions, monies were deposited into a CDC by a drug trafficking organization. Using false identities, the CDC then wired that money through its Wachovia correspondent bank accounts for the purchase of airplanes for drug trafficking organizations. On various dates between 2004 and 2007, at least four of those airplanes were seized by foreign law enforcement agencies cooperating with the United States and were found to contain large quantities of cocaine.

10. In total, nearly $13 million dollars went through correspondent bank accounts at Wachovia for the purchase of aircraft to be used in the illegal narcotics trade. From these aircraft, more than twenty thousand kilograms of cocaine were seized.

Wachovia's CDC Business Was High Risk

11. The account holders at Wachovia that conducted these transactions were Mexican CDCs. A CDC is not a bank. CDCs are licensed non-bank currency exchange businesses that are located in a number of countries, including Mexico. CDCs allow persons in Mexico to exchange one type of currency for other currency, *e.g.,* exchange a value of pesos for an equal value of U.S. dollars or a value of U.S. dollars for an equal value of pesos. Through CDCs, persons in Mexico can use hard currency, such as pesos or U.S. dollars, and wire transfer the value of that currency to U. S. bank accounts to purchase items in the United States or other countries.

12. CDCs do not operate in the same manner as banks operate in the United States. CDCs do not hold deposits or maintain checking accounts, savings accounts, or issue lines of credit. Nor do CDCs provide personal and/or commercial banking services. A central function of CDCs is to allow persons or businesses in Mexico to exchange or wire transfer the value of hard currency from Mexico to bank accounts in the United States or other countries to conduct commerce.

13. The nature of the CDC business allows money launderers the opportunity to move drug dollars that are in Mexico into CDCs and ultimately into the U. S. banking system. Once the drug dollars were placed into CDCs, they were readily wire transferred into bank accounts of CDCs at Wachovia.

14. Wachovia maintained correspondent bank accounts for a number of Mexican CDCs. The Wachovia business unit that managed and oversaw the CDC business was located in Miami, Florida. Miami has been designated as both a High Intensity Money Laundering and Related Financial Crime Area and a High Intensity Drug Trafficking Area. In 2005, Mexico also was designated as a high-risk source of money laundering activity, particularly the financial activities through CDCs. The CDCs involved in the movement of drug monies in this

investigation were all based in Mexico.

15. As early as 1996, the DEA, federal regulators and other prominent anti-money laundering organizations began publicly highlighting the increased money laundering risk presented by Mexican CDCs to the U.S. financial system. The DEA warned that Mexican drug trafficking organizations were increasingly using CDCs to place drug proceeds into the U.S. financial system by smuggling the drug proceeds out of the United States to Mexico and selling those dollars to Mexican CDCs for pesos. The placement of drug proceeds with Mexican CDCs is beneficial to both sides of the transaction: the drug trafficking organization is able to obtain local currency (pesos) to continue its illicit activities without having to risk structuring drug proceeds into the banking system, and the CDCs, which have a significant need for U.S. dollars in the ordinary course of their currency exchange activities, obtain a valuable source of discounted U.S. dollars.

16. In addition to the above warnings, in April of 2006, FinCEN warned the U. S. banking and financial industry of potential misuse of correspondent banking relationships with Mexican CDCs. FinCEN specifically warned that the repatriation of bulk cash, multiple wire transfers initiated by CDCs remitting funds to jurisdictions outside of Mexico that bear no apparent business relationship with the CDC, and the deposit of third-party items, including sequentially numbered monetary instruments, were all activities that could be associated with money laundering.

17. As early as 2004, Wachovia understood the risk that was associated with doing business with the Mexican CDCs. Wachovia was aware of the general industry warnings. As early as July 2005, Wachovia was aware that other large U. S. banks were exiting the CDC business based on AML concerns.

18. Despite these warnings, Wachovia remained in the business. And in September 2005, Wachovia purchased the right to solicit the international correspondent banking customers of Union Bank of California ("UBOC"). Wachovia knew that UBOC was exiting the CDC market due to AML problems. Wachovia hired at least one person from UBOC who had a significant role in the CDC business at UBOC. After UBOC exited the CDC business, Wachovia's business volume increased notably.

The Nature of Wachovia's CDC Business

19. From September 2005 to December 2007, Wachovia provided correspondent banking services to 22 CDCs, including Casa de Cambio Puebla.

20. Wachovia offered the CDCs at least three services. First, Wachovia allowed CDCs to conduct wires through Wachovia. These wires were sent by the CDC on behalf of its third-party customers, who were in Mexico, to recipients throughout the world.

21. Second, Wachovia offered a "bulk cash" service to CDCs. Using this service, CDCs collected large amounts of U. S. dollars in Mexico. Those dollars, or "bulk cash," would then be physically transported to the United States from the CDC either through an armored car service or through a means designated by the CDC. Once in the United States, the money would ultimately be deposited at the Federal Reserve. Through this method, CDCs could repatriate U.S. dollars into the U.S. market.

22. Third, Wachovia offered a pouch deposit service to the CDCs. The CDCs would accept deposit items drawn on U.S. banks, *e.g.*, checks and traveler's checks presented by their customers. Those items would then be aggregated and placed into a "pouch" that would be forwarded to Wachovia in the United States for deposit. In or around May 2005, Wachovia introduced a new delivery method for international check deposits called "remote deposit capture" ("RDC"). RDC allowed the CDCs to scan the individual deposit items into a digital format. The scanned files then would be forwarded electronically to Wachovia for credit.

23. The CDCs that banked at Wachovia conducted significant wire, bulk cash, and "pouch" or RDC activity through Wachovia. For the time period of May 1, 2004 through May 31, 2007, Wachovia processed at least $373,630,892,102 in wire activity on behalf of the CDCs. During that same time period, Wachovia processed at least $4,728,626,300 in bulk cash for the CDCs. For the same time period, Wachovia processed approximately $47,000,000,000 in RDC deposits for all of its correspondent banking customers, which included the Mexican CDCs.

Suspicious Activity and Drug Money Laundering Through the CDC Accounts

24. During the investigation, law enforcement reviewed the CDC banking activity that occurred at Wachovia and found readily identifiable evidence and red flags of large-scale drug money laundering. A small representation of that conduct includes:

1. Structured Wire Transactions: It was commonplace in the CDC accounts for multiple round-number wires to be made on the same day or in close succession, by the same wire senders, for the benefit of the same account.

   For example, over a two-day period, ten wire transfers by four different individuals and one business went through Wachovia for deposit into an aircraft broker's escrow account. All of the transfers were in round numbers. None of the individuals or business that wired the money had any connection to the aircraft or to the entity that allegedly owned the aircraft. The investigation has further revealed that the identities of the individuals who sent the money were false and that the business was a shell entity. That plane was subsequently seized with approximately 2000 kilograms of cocaine aboard.

   On another occasion, a CDC sent eight wires through Wachovia for deposit into an

aircraft broker's account on the same day. Four of those wires were allegedly sent by one individual; two wires were for $49,000 and two wires were for $51,000. The remaining four wires were allegedly sent by another individual; each of the four wires was for $50,000. The next day, another CDC sent ten wires through Wachovia to the same plane broker's account. Each wire was for $50,000. All of this money was intended for the purchase of an aircraft, but the money was seized by law enforcement before the deal was completed. The investigation has further revealed that the identities of the individuals who sent the money were false.

On another occasion, over a seven-day period, a CDC sent more than $1.3 million in wire transfers through Wachovia for deposit into a plane broker's accounts. There were a total of fifteen wires, and they ranged in amount from $63,000 to $127,500 dollars. All of this money was intended for the purchase of an aircraft, but the money was seized by law enforcement before the deal was completed.

2. Sequentially Numbered Traveler's Checks That Contained Unusual Markings: The CDCs regularly deposited traveler's checks through pouch deposits that contained numerous examples of structuring, sequential serial numbers and endorsement/deposit dates on or near the date of purchase. Other suspicious elements included "smurf marks," or unusual markings, and traveler's checks that lacked any legible signature.

3. Significant Bulk Cash Transactions In Great Excess of A Customer's Self-Identified Expectations: Many of the CDCs that used Wachovia's bulk cash service sent significantly more cash to Wachovia than what Wachovia had expected. More specifically, many of the CDCs exceeded their expected monthly activity by at least 50 percent.

The BSA Investigation

25. Recognizing these red flags, in May 2007, the United States Attorney's Office for the Southern District of Florida, the IRS, and the DEA began investigating Wachovia's BSA compliance program. FinCEN subsequently joined the investigation. The OCC conducted a parallel examination.

26. These BSA investigations have determined that from May 2003 through at least July 2007, Wachovia violated the anti-money laundering ("AML") and suspicious activity reporting requirements of the BSA and its implementing regulations. The violations at Wachovia were serious and systemic and allowed certain Wachovia customers to launder millions of dollars of proceeds from the sale of illegal narcotics through Wachovia accounts over an extended time period.

27. The investigation has identified at least $110 million in drug proceeds that were funneled

through the CDC accounts held at Wachovia. Wachovia failed to appreciate and address the risks associated with its Mexican CDC customer base and failed to recognize that its BSA/AML program was inadequate for the task of monitoring for suspicious transactions from the CDCs.

28. The investigation has determined that there were essentially seven significant failures in Wachovia's AML and Compliance programs:

A. Lack of policies, procedures, or monitoring controls governing the repatriation of nearly $14 billion of United States dollars in bulk cash for high-risk CDCs and other foreign correspondent bulk cash customers;

B. Failure to conduct monitoring of over $40 billion in monetary instruments flowing through international foreign correspondent accounts in the form of RDC for a two-year period;

C. Failure to conduct adequate levels of due diligence of high-risk CDC customers;

D. Failure to adequately monitor CDCs and other high-risk foreign correspondent banking accounts in order to fulfill suspicious activity reporting obligations;

E. Failure to implement monitoring controls or limits for sequentially numbered traveler's checks for high-risk CDC customers in contravention of Wachovia's policy;

F. Failure to detect and report suspicious activity in a timely manner on the $373 billion in wire transfers that were processed by Wachovia for the CDCs; and

G. Failure to implement effective BSA/AML audit coverage.

Due Diligence and Monitoring of CDC and Correspondent Account Activity

29. Federal banking regulators have advised banks, including Wachovia, that an effective AML program should be risk-based and incorporate the following principles into their business practices:

A. Determine the true identity of all customers requesting services;

B. Determine the particular customer's source(s) of funds for transactions;

C. Determine the particular customer's normal and expected transactions;

D. Monitor customer transactions to determine if they are consistent with the

normal and expected transactions for that customer or for similar categories or classes of customers;

E. Identify customer transactions that do not appear to be consistent with normal and expected transactions for that particular customer or for customers in similar categories or classes; and

F. Determine if transactions are unusual or suspicious and, if so, report those transactions.

The business practices listed above are commonly referred to in the industry and by law enforcement as the "Know Your Customer" ("KYC") requirements.

30. Although the bank collected information relating to the identities of its CDC customers, the expected source of funds, and the normal or expected transactions, this information was not disseminated to the AML employees and was not readily available when AML was conducting investigations of transactions. Nor was there any critical analysis of actual account activity against the expected activity.

31. The bulk of the correspondent and CDC banking activity involved wire activity. This wire activity was principally monitored through the use of a computer system. The computer system would generate monthly alerts based on parameters established by Wachovia. Those alerts were then to be investigated for potential suspicious activity by the AML personnel in the Philadelphia, Pennsylvania office of Wachovia. Wachovia's wire monitoring, however, was not commensurate with the risk posed by the CDCs. The level of scrutiny imposed on the wire transactions was significantly limited by personnel and budgetary concerns. The actual number of alerts that the system was designed to generate per month was pre-set, based, in part, on the number of investigators available to review the alerts. In addition, AML personnel were not allowed to carry investigations into the next month. As a result, any investigation that was begun in one month had to be completed within the same month. The net result was that the understaffed AML unit in Philadelphia could not keep up with the volume of wires. The suspicious activity went effectively unmonitored. The $373 billion in CDC wire transfers were monitored in this inadequate manner.

Bulk Cash

32. With regard to the bulk cash business, Wachovia had no written formal AML policy or procedure for the monitoring of bulk cash to ensure that suspicious activity was reported. AML and compliance personnel did not examine or review the denominations or the regional source of the bulk cash to compare it against known trends and customer expectations. Wachovia also did not compare the monthly total amount of repatriated bulk currency money against customer expectations. Thus, although Wachovia recorded expected activity in bulk cash for each of its customers, no AML or compliance personnel ensured that the actual

customer activity matched the customer expectations. As a result, at least $4,728,626,300 in bulk cash from the CDCs went through Wachovia during the period of May 1, 2004 through May 31, 2007, with essentially no AML monitoring.

Remote Deposit Capture and Pouch Activity

33. Wachovia never reviewed any of the RDC deposits made from the time the product was first offered in the summer of 2005 until approximately November 2007. During this time, approximately $47 billion was deposited into Wachovia through RDC without AML monitoring. These deposits included traveler's checks, third party checks, money orders, and other negotiable instruments. Thus, none of these instruments were subject to examination for "smurfing," structuring, or other common money laundering techniques associated with these types of instruments.

34. With regard to standard pouch activity, Wachovia also failed to enforce a self-imposed policy regarding traveler's checks. In 2005, Wachovia was warned that the CDCs were sending in large quantities of sequentially numbered traveler's checks for deposit and that this was potentially suspicious activity. As a result of this warning and other internal discussions, Wachovia sent a letter to its customers noting that, "due to the strict U.S. regulatory mandates associated with anti-money laundering policies, Wachovia has decided to limit acceptance of bulk deposits of traveler's checks through our cash letter service." The letter stated that Wachovia "will require that you no longer remit deposits containing sequentially numbered USD traveler's checks where the total value of the series exceeds $10,500." Wachovia, however, failed to establish any internal policy or monitoring procedures to implement or enforce this rule. As a result, from April 2005 through May 2007, Wachovia accepted more than 1000 pouch deposits that contained thousands of sequentially numbered traveler's checks in violation of its own policy.

In addition, Wachovia's methodology of review of the pouch activity did not occur in "real time" or near "real time." Oftentimes, because of budgetary and/or staffing concerns, the deposit items would be examined three to six months after the deposit had occurred. As a result, any resulting suspicious activity report would relate to dated transactions.

35. As a result of these failures, and as a result of Wachovia's internal audits not identifying these failures, a voluntary transaction review undertaken by Wachovia indicates that from April 1, 2005 through May 31, 2007, 13 of the Mexican CDCs processed more than $20,000,000 in sequentially numbered traveler's checks through Wachovia in violation of Wachovia's own policy. The majority of those traveler's checks contained no legible names. Approximately 64% of those traveler's checks contained unusual markings, that is, markings that were either handwritten or stamped and included numbers, letters, or a combination of both. Such markings, lack of signatures, and the sequential numbering of checks are readily identifiable patterns of money laundering activity.

Wachovia's Considerable Cooperation and Remedial Actions

36. Since the beginning of the BSA investigation, Wachovia has fully cooperated and has provided valuable assistance to law enforcement. Wachovia retained an outside law firm to assist in investigating the facts relevant to the United States' investigation. With the assistance of outside counsel, Wachovia has made numerous detailed periodic reports to the United States concerning those facts.

37. Wachovia has devoted substantial resources to that investigation and to responding to the United States' requests for information. To date, Wachovia has produced more than 8 million pages of documents. Wachovia has organized its document productions as requested by the United States and has provided summaries, indices, and explanations of relevant documents to assist the United States in its understanding of the facts relevant to its investigation. Wachovia has also made employees available to be interviewed by the United States as requested.

38. Wachovia has also taken extensive remedial measures to address any shortcomings in its BSA/AML programs.

a. In June 2007, Wachovia hired a new Chief Compliance Officer. In April 2008, Wachovia also hired a new BSA/AML Officer.

b. Under the leadership of the new Chief Compliance Officer and the new BSA/AML Officer, Wachovia undertook a substantial remediation of its AML and compliance functions.

c. Wachovia enhanced its manual transactional party monitoring, with focuses on high-risk countries and financial institution risk.

d. Wachovia developed and provided enhanced AML training for employees, including AML Investigative Services staff. Topics of training have included regulatory responsibility, red flag detection, the black market peso exchange, large cash transactions, wires to high-risk countries, and activity inconsistent with an account's stated purpose.

39. Wachovia voluntarily conducted a detailed "lookback" of Wachovia's transactions with thirteen Mexican CDCs during a three-year period. Wachovia has provided the results of the lookback, which was conducted by an independent consultant, to the United States and its banking regulators. As a result of the "lookback" program, Wachovia has filed SARs for conduct related to the CDCs.

A. Wachovia filed more than 4200 SARs relating to wire transactions conducted by the CDCs, which included $4.3 billion in total dollars;

B. Wachovia filed 8 SARs relating to bulk cash transactions conducted by the CDCs, which included $4,011,256,648 in total dollars;

C. Wachovia filed 18 SARs relating to sequentially numbered traveler's check transactions conducted by the CDCs, which included $23,155,000 in total dollars.

40. Since Wachovia's acquisition by Wells Fargo, Wachovia has been subject to Wells Fargo's BSA/AML Compliance Program and compliance and operational risk management, oversight, and independent testing. Wells Fargo's policies and procedures, including those relating to escalation and exiting of customer relationships, now apply to Wachovia. As the integration progresses, Wells Fargo's transaction monitoring system, a more advanced version of the system used by Wachovia, will be used to monitor Wachovia's transactions.

The Asset Forfeiture and Money Laundering Section Investigation

41. From 2003 to 2008, Wachovia Bank maintained account relationships with certain third-party payment processors.

Telemarketing Practices and Third-Party Payment Processors

42. Telemarketers engaged in deceptive sales calls during which they obtained individuals' bank account information and subsequently transmitted that information to third-party payment processors. Wachovia Bank processed remotely-created checks ("RCCs") as part of its relationship with certain payment processors. Unlike a personal check, where the payor signs his or her name for authorization, RCCs include text such as "authorized by your depositor." The RCCs were deposited into the payment processors' accounts at Wachovia and then drawn on the personal accounts of individual customers of the merchant-clients. The processors then sent the deposited funds to the telemarketers via domestic and international wire transfers.

43. The individual customers or their financial institutions returned many of these RCCs to the payment processors' accounts at Wachovia, complaining that a high number of the RCCs were not authorized by the customers on whose accounts they were drawn. In many instances, the volume of returns was high -- in some cases exceeding 40% of the deposited RCCs – and the reason listed for some of the returned RCCs was "unauthorized." Despite the fact that Wachovia received information from both internal and external sources about the volume of returns and the reasons for the returns, the payment processors' accounts were left open. Wachovia profited from fees it charged the payment processors to process returned RCCs. During the relevant time period, PPC, Suntasia and YMA/Netchex deposited approximately $418 million into Wachovia accounts.

Due Diligence and Monitoring of Payment Processor Accounts

44. Wachovia failed to develop and maintain an effective risk-based BSA/AML compliance program in light of the inherent risks associated with third-party payment processors and

their high-risk services. The third-party payment processors were high-risk because they conducted off-shore wire transfers to/from high-risk countries. Third-party payment processors also presented an elevated risk because their accounts experienced high return rates. Despite these risk indicators, Wachovia failed to develop a program to analyze the third-party payment processor accounts commensurate with the risks they presented.

45. In particular, the Bank failed to (1) request detailed information about payment processors' merchant base and major customers; (2) have a detailed understanding of the processors' charge-back history; and (3) sufficiently scrutinize the processors' due diligence programs. Moreover, where Wachovia did identify telemarketers referenced in a state cease and desist order, Wachovia notified the processor but did not confirm the assurances it received from the processor that it no longer processed for the telemarketers. Also, Wachovia did not determine overall return rates for RCCs and the rates for specific return reasons. Had Wachovia properly monitored return rates and the reasons for returns, the monitoring would have resulted in multiple red flags. In addition, Wachovia failed to develop a process or procedure to monitor the processors' wire activity. While Wachovia filed SARs on the payment processors' account activity, those SARs did not cover all suspicious wire activity in those accounts, some of which involved entities located in high-risk countries. Moreover, with respect to one of the payment processors, Wachovia failed to close the processor's accounts after identifying three instances of suspicious activity.

46. Wachovia assigned due diligence and KYC responsibilities to its relationship managers. Delegating these responsibilities to relationship managers allowed the business unit to decide whether to call for additional due diligence. The payment processors' accounts should have been classified as high-risk and subjected to additional due diligence. Although Wachovia's enhanced due diligence unit reviewed one of the payment processor's accounts, Wachovia's overall KYC process failed to include critical elements such as an examination of sources of wealth, an examination of international transactions, or an examination of changes in account activity.

Termination of Accounts

47. After additional information was received and the Government's action in United States v. PPC, No. 06-725 (E.D. Pa. filed Feb. 17, 2006), which froze certain payment processors' accounts at Wachovia based on allegations that PPC's merchant-clients were defrauding their customers, Wachovia examined its relationships with payment processors. Wachovia was subsequently the subject of investigations by the Department of Justice and OCC and of civil class action suits regarding these relationships. In response, Wachovia began terminating its relationships with third-party payment processors. Wachovia subsequently instituted remedial measures to enhance its fraud-detection and compliance capabilities with respect to telemarketers, payment processors, and other customers that create RCCs. Wachovia has also funded a restitution program to reimburse individuals whose RCCs were deposited by the payment processors.