UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO. _____**
	:	
v.	:	**VIOLATIONS: 18 U.S.C. § 371**
	:	**(Conspiracy to Violate IEEPA);**
COMMERZBANK AG, and	:	**31 U.S.C. §§ 5318(g), 5318(h),**
COMMERZBANK AG NEW YORK	:	**5318(i), and 5322(b)**
BRANCH,	:	**(Violations of the BSA)**
	:	
Defendants.	:	**FORFEITURE: 21 U.S.C. § 853(p); 18**
	:	**U.S.C. § 981(a)(1)(C); and 28 U .S.C.**
	:	**§ 2461(c)**

INFORMATION

The United States charges that:

General Allegations

1. At all times relevant to this Information Defendant, Commerzbank AG, ("COMMERZ") was a financial institution registered and organized under the laws of Germany.

2. Since in or about 1971, and at all times relevant to this Information, COMMERZ had a license issued by the state of New York to operate as a foreign bank branch in New York, New York.

3. At all times relevant to this Information, COMMERZ conducted U.S. Dollar ("USD") clearing at Defendant Commerzbank AG New York Branch ("COMMERZ NEW YORK"), which was located in Manhattan, New York.

4. At all times relevant to this Information, COMMERZ and COMMERZ NEW YORK were subject to oversight and regulation by the Board of Governors of the Federal Reserve, including the Federal Reserve Bank of New York ("FRBNY"), as well as the New York State Department of Financial Services ("DFS").

5. At all times relevant to this Information, COMMERZ had branches throughout the world and conducted financial transactions in USD at and through COMMERZ NEW YORK and unaffiliated U.S. financial institutions in New York and elsewhere.

The International Emergency Economic Powers Act

6. The United States Department of the Treasury, Office of Foreign Assets Control ("OFAC"), which is located in the District of Columbia, among other things, administers and enforces economic and trade sanctions against certain foreign countries and entities associated with those countries, including institutions located in or controlled by Sudan and Iran ("Sanctioned Entities"). At all relevant times, OFAC was empowered to authorize transactions with institutions located in, or controlled by, these countries by granting licenses for transactions. In addition, OFAC administers and enforces economic and trade sanctions against Specially Designated Nationals ("SDNs").[1]

7. Over the years, the United States has employed sanctions and embargos with regard to Sanctioned Entities and SDNs. Those restrictions arose, in part, in response to repeated support by those nations and entities for international terror against the United States and its allies and, with regard to Iran, the proliferation of weapons of mass destruction.

8. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706, authorized the President of the United States (the "President") to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declared a national emergency with respect to that threat. Pursuant to the authority under IEEPA, the

[1] OFAC publishes a Specially Designated National ("SDN") List, which includes individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and weapons of mass destruction proliferators designated under programs that are not country-specific.

President and the executive branch have issued orders and regulations governing and prohibiting certain transactions with Iran by U.S. persons or involving U.S.-origin goods.

9. Pursuant to 50 U.S.C. §1705, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under IEEPA.

The Iranian Sanctions

10. On March 15, 1995, President William J. Clinton issued Executive Order No. 12957, finding that "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and declaring "a national emergency to deal with that threat."

11. President Clinton followed this with Executive Order No. 12959, issued on May 6, 1995, which imposed comprehensive trade and financial sanctions on Iran. These sanctions prohibit, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Iran or the Government of Iran of any goods, technology, or services from the United States or by U.S. persons, wherever located. This includes persons in a third country with knowledge or reason to know that such goods, technology, or services are intended specifically for supply, transshipment, or re-exportation, directly or indirectly, to Iran or the Government of Iran. On August 19, 1997, President Clinton issued Executive Order No. 13059, consolidating and clarifying Executive Order Nos. 12957 and 12959 (collectively, the "Executive Orders"). The Executive Orders authorized the U.S. Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary

of the Treasury promulgated the Iranian Transaction Regulations ("ITRs"),[2] 31 C.F.R. Part 560, implementing the sanctions imposed by the Executive Orders.

12. With the exception of certain exempt transactions, the ITRs prohibit, among other things, U.S. depository institutions from servicing Iranian accounts and directly crediting or debiting Iranian accounts. One such exception would be transactions for which a validated export license had been obtained from OFAC, which was located in the District of Columbia. The ITRs also prohibit transactions that evade or avoid, have the purpose of evading or avoiding, or attempts to evade or avoid the restrictions imposed under the ITRs. The ITRs were in effect at all times relevant to the conduct described below.

13. While the ITRs promulgated for Iran prohibited USD transactions, they contained a specific exemption for USD transactions that did not directly credit or debit a U.S. financial institution. This exemption is commonly known as the "U-turn exemption."

14. The U-turn exemption permitted banks to process Iranian USD transactions that began and ended with a non-U.S. financial institution, but were cleared through a U.S. correspondent bank. In relevant part, the ITR provided that U.S. banks were "authorized to process transfers of funds to or from Iran, or for the direct or indirect benefit of persons in Iran or the Government of Iran, if the transfer . . . is by order of a foreign bank which is not an Iranian entity from its own account in a domestic bank . . . to an account held by a domestic bank . . . for a [second] foreign bank which is not an Iranian entity." 31 C.F.R. §560.516(a)(1). That is, a USD transaction to or for the benefit of Iran could be routed through the United States as long as a non-U.S. offshore bank originated the transaction and the transaction terminated with a non-U.S. offshore bank. These U-turn transactions were only permissible where no U.S. person or

---

[2] Effective October 22, 2012, the Department of the Treasury renamed and reissued the ITR as the Iranian Transactions and Sanctions Regulations.

entity had direct contact with the Iranian bank or customer and were otherwise permissible (e.g., the transactions were not on behalf of an SDN).

15. Effective November 10, 2008, OFAC revoked the U-turn exemption for Iranian transactions. As of that date, U.S. depository institutions were no longer authorized to process Iranian U-turn payments.

The Sudanese Sanctions

16. On November 3, 1997, President Clinton issued Executive Order No. 13067, which imposed a trade embargo against Sudan and blocked all property and interests in property of the Government of Sudan. Effective July 1, 1998, OFAC issued the Sudanese Sanctions Regulations ("SSR"), 31 C.F.R. Part 538, to implement Executive Order No. 13067. On October 13, 2006, President George W. Bush issued Executive Order No. 13412 (collectively with Executive Order No. 13067, the "Sudanese Executive Orders"), which continued the comprehensive blocking of the Government of Sudan imposed by Executive Order No. 13067, but exempted the then-regional Government of South Sudan from the definition of the Government of Sudan. The Sudanese Executive Orders prohibit virtually all trade and investment activities between the United States and Sudan, including, but not limited to, broad prohibitions on: (i) the importation into the United States of goods or services from Sudan; (ii) the exportation or re-exportation of any goods, technology, or services from the United States or by a U.S. person to Sudan; and (iii) trade- and service-related transactions with Sudan by U.S. persons, including financing, facilitating, or guaranteeing such transactions. The Sudanese Executive Orders further prohibited "[a]ny transaction by any U.S. person or within the U.S. that evades or avoids, or has the purposes of evading or avoiding, or attempts to violate, any of the prohibitions set forth in [the SSR]." With the exception of certain exempt or authorized

transactions, OFAC regulations implementing the Sudanese sanctions generally prohibited the export of services to Sudan from the United States.

The Bank Secrecy Act

17. The Currency and Foreign Transactions Reports Act of 1970, as amended (commonly known as the Bank Secrecy Act, or "BSA"), 31 U.S.C. § 5311, et seq., and its implementing regulations require domestic banks, domestic branches of foreign banks, and certain other financial institutions to establish and maintain programs designed to detect and report suspicious activity, and to maintain certain related records "where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 31 U.S.C. § 5311.

18. Among other things, the BSA requires that financial institutions "maintain appropriate procedures to ensure compliance with [the BSA] and regulations prescribed under [the BSA] or to guard against money laundering." 31 U.S.C. § 5318(a)(2). Pursuant to 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1020.210, COMMERZ and COMMERZ NEW YORK, the defendants, were required to establish and maintain an anti-money laundering ("AML") compliance program that, at a minimum:

a. provided internal policies, procedures, and controls designed to guard against money laundering;

b. provided for a compliance officer to coordinate and monitor day-to-day compliance with the BSA and AML requirements;

c. provided for an ongoing employee training program; and

d. provided for independent testing for compliance conducted by bank personnel or an outside party.

19. In addition, the BSA requires financial institutions to "report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1).

Pursuant to 31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320(a)(2), a financial institution is required to file a Suspicious Activity Report ("SAR") when it "knows, suspects, or has reason to suspect" that a transaction, among other things, involves funds derived from illegal activities or has no apparent business or lawful purpose.

20. The BSA also requires financial institutions that establish, maintain, administer, or manage correspondent accounts in the United States for non-United States persons to establish "appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts." 31 U.S.C. § 5318(i)(1). Pursuant to 31 U.S.C. § 5318(i) and 31 C.F.R. § 1010.610, a financial institution is required to conduct "enhanced scrutiny" of any correspondent account, including any such account maintained for foreign branches or affiliates of that financial institution, "to guard against money laundering and to identify and report any suspicious transactions."

COUNT ONE

(CONSPIRACY TO VIOLATE THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT)

21. The allegations contained in paragraphs 1 through 16 above are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

22. From in or around January 2002 through in or around December 2008, COMMERZ facilitated USD transactions for a number of Sanctioned Entities and SDNs. At no time did COMMERZ or its co-conspirators apply for, receive, or possess a license or authorization from OFAC for any of the criminal conduct set forth below.

The Conspiracy and Its Objects

23. From in or around January 2002 through in or around December 2008, the exact dates being unknown to the United States, in the District of Columbia and elsewhere, Defendant

COMMERZBANK AG

and others, both known and unknown to the United States, unlawfully, willfully and knowingly combined, conspired, confederated and agreed with one another and with others to commit offenses against the United States, that is, to engage in financial transactions with Sanctioned Entities and SDNs in violation of IEEPA, and the executive orders and regulations issued thereunder.

Goals of the Conspiracy

24. The goal of the conspiracy was for COMMERZ and others, both known and unknown to the United States, to enrich themselves by engaging in a conspiracy and a scheme to violate IEEPA, and the executive orders and regulations issued thereunder.

25. A further goal of the conspiracy was for COMMERZ and others both known and unknown to the United States, to violate executive orders and regulations prohibiting the exportation, directly and indirectly, of services from the United States to Sanctioned Entities and SDNs.

Manner and Means of the Conspiracy

26. Among the manner and means by which COMMERZ and its co-conspirators carried out the conspiracy were the following:

a. COMMERZ intentionally used a non-transparent method of payment messages, known as cover payments, to conceal the involvement of Sanctioned Entities and SDNs in USD transactions processed through COMMERZ NEW YORK and other financial institutions in the United States.

b. COMMERZ instructed other financial institutions not to mention the names of Sanctioned Entities in USD payment messages sent to COMMERZ NEW YORK and other financial institutions in the United States.

c. COMMERZ followed instructions from Sanctioned Entities and SDNs not to mention their names in USD payment messages sent to COMMERZ NEW YORK and other financial institutions in the United States.

d. COMMERZ removed information identifying Sanctioned Entities from USD payment messages in order to conceal the involvement of Sanctioned Entities from COMMERZ NEW YORK and other financial institutions in the United States.

e. COMMERZ and an Iranian company processed transactions through special purpose entities to conceal the Iranian client's involvement in the transactions, and to prevent the transactions from being blocked or rejected in the United States. COMMERZ and the client switched use of such special purpose entities when COMMERZ NEW YORK's United States sanctions compliance filters were updated to detect the use of a particular special purpose entity.

Overt Acts

27. In furtherance of the conspiracy and to achieve the objects and purposes thereof, COMMERZ and co-conspirators, both known and unknown to the United States, committed and caused to be committed, in the District of Columbia and elsewhere, the following overt acts, among others:

a. In or around 2002, a group within COMMERZ's head office in Frankfurt implemented a procedure that applied only to payment messages for Iranian entities transiting through the United States to ensure that the payment messages did not mention the Iranian ordering party. This procedure existed because if the text were not changed the payments might be stopped, rejected, or blocked due to U.S. sanctions.

b. In or around June 2004, COMMERZ employees and employees of an Iranian Bank, had agreed that in lieu of sending direct wire payments to beneficiaries in the United States (in violation of U.S. sanctions), the Iranian Bank would pay U.S. beneficiaries, using checks that listed only the Iranian Bank's address in London.

c. In or around March 2005, the Hamburg branch of COMMERZ created a "safe payment solution" on behalf of an Iranian company that involved routing payments through sub-entities controlled by the Iranian company. These sub-entities were incorporated outside of Iran and bore no obvious connection to the Iranian company. The Hamburg branch of COMMERZ charged more for payments sent using the "safe payment solution" than it did for normal foreign payments.

d. From on or about September 10, 2008, through on or about December 31, 2008, COMMERZ processed payments on behalf of entities that it knew to be owned or controlled by an Iranian company that had been designated on or about September 10, 2008, as an SDN by OFAC for its involvement in weapons of mass destruction proliferation.

e. In or around August 2001, COMMERZ advised one of its Sudanese bank clients that in order to evade U.S. sanctions in the course of conducting USD transactions, the Sudanese bank should send its transactions using the cover payment method to COMMERZ NEW YORK. COMMERZ further advised its Sudanese bank client that its cover payments should not contain any references to the Sudanese origin of the payments.

(Title 18, United States Code, Section 371.)

COUNT TWO

(Violation of the Bank Secrecy Act:
Failure to Maintain an Effective Anti-Money Laundering Program)

The United States further charges:

28. The allegations contained in paragraphs 1 through 20, 22, and 24-27 above are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

29. From at least in or about 2008, and continuing until at least in or about 2013, COMMERZ NEW YORK violated the BSA and its implementing regulations. Specifically, COMMERZ NEW YORK failed to maintain adequate policies, procedures, and practices to ensure its compliance with United States law, including their obligation to detect and report suspicious activity. As a result of the willful failure of COMMERZ NEW YORK to comply with United States law, a multi-billion dollar securities fraud was operated through COMMERZ and COMMERZ NEW YORK.

The Olympus Accounting Fraud

30. At all times relevant to this Information, the Olympus Corporation ("Olympus") was a Japanese-based manufacturer of medical devices and cameras. Its common stock is listed on the Tokyo Stock Exchange, and its American Depository Receipts trade in the United States.

31. From at least in or about the late 1990s through in or about 2011, Olympus perpetrated a massive accounting fraud designed to conceal from its auditors and investors hundreds of millions of dollars in losses. In September 2012, Olympus and three of its senior executives pleaded guilty in Japan to inflating the company's net worth by approximately $1.7 billion.

32. Olympus used COMMERZ, through its private banking business in Singapore, known as Commerzbank (Southeast Asia) Ltd. ("COSEA"), and a trusts business in Singapore,

Commerzbank International Trust (Singapore) Ltd. ("CITS), and COMMERZ NEW YORK, through its correspondent banking business, to perpetrate its fraud. COMMERZ, through its branch and affiliates in Singapore, both loaned money to off-balance-sheet entities created by or for Olympus to perpetrate its fraud, and transacted more than $1.6 billion through COMMERZ NEW YORK in furtherance of the fraud.

The Suspicions at COMMERZ

33. COMMERZ and COMMERZ NEW YORK were used in furtherance of the Olympus fraud during two different time periods. From approximately in or about 1999 through in or about 2000, COMMERZ and its Singapore branch and affiliates were one of the primary banks through which the fraud was operated.

34. During that time period, Olympus executives asked executives from CITS to provide certain false documents to Olympus's auditors, which would have failed to disclose that certain Olympus assets were pledged as collateral for loans from COSEA. CITS obtained a legal opinion, which, in the words of one CITS executive written to an Olympus executive, "makes clear that our bank could be subject to both civil and criminal penalties if we are seen to be assisting or facilitating you in the non-disclosure." Although CITS ultimately declined to provide the false documents, its executives suggested a variety of ways in which Olympus could nonetheless fail to disclose the pledge.

35. In or about 2000, Olympus took its business away from CITS and COSEA and to another bank. In or about 2005, however, Olympus – and its fraud – returned to CITS and COSEA. From at least 2008 until at least in or about 2010, CITS and COSEA executives expressed strong suspicions about the Olympus transactions and structure. One senior executive worried that Olympus would have to "write off [the] full amount" of the relevant transactions, and wondered about the effects on CITS if "any negative news is splash[ed] on the front page."

Similarly, a senior legal and compliance officer responsible for COMMERZ's Singapore branch and affiliates wrote at the time that he was "concerned about fraud, asset stripping, market manipulation and derivative Tax offenses. . . . If the [Olympus] structure and transactions cannot [be] explained we must file Suspicious Transaction report as a matter of law and [COMMERZ] policy." Other Singapore-based compliance officers wrote about the Olympus business that it was "a very complicated structure without any economical rationale."

36. Another senior compliance officer - who would later become head of compliance at COMMERZ NEW YORK – internally reported that a senior Singapore-based executive at CITS had stated that "he did not typically ask questions of clients as he felt he was at less risk by not knowing." The compliance officer responded by "repeat[ing] that it is unacceptable for senior managers to turn blind eyes or otherwise remain ignorant."

The New York Wires

37. In or about March 2010, two wires in the amounts of approximately $455 million and $67 million, respectively, related to the Olympus scheme were processed by COMMERZ NEW YORK through the correspondent account for the Singapore branch of COMMERZ. Those wires caused COMMERZ NEW YORK's automated AML monitoring software to "alert."

38. At the time, COMMERZ NEW YORK had conducted no due diligence on the Singapore branch, consistent with COMMERZ's policy at that time. In response to the alerts, however, COMMERZ NEW YORK sent a request for information to COMMERZ Frankfurt and COMMERZ's Singapore branch, inquiring about the transactions. The Singapore branch responded in a brief e-mail, dated April 20, 2010, referring to the Olympus-related entities involved in the wires:

> GPA Investments Ltd. ist [*sic*] a Cayman Islands SPV, Creative Dragons SPC-Sub Fund E is a CITS administered fund both of

> which are part of an SPC structure to manage securities investments for an FATF country based MNC.
>
> According to the Relationship Manager the payment reflects the proceeds from such securities investments to be reinvested.

COMMERZ's Singapore branch did not relay any of the concerns about the Olympus-sponsored structures and transactions.

39. Based on its response, COMMERZ NEW YORK closed the alert without taking any further action other than to note that in March 2010 alone, GPA Investments had been involved in six transactions through COMMERZ NEW YORK totaling more than $522 million. In fact, between 1999 and 2010, a total of more than $1.6 billion in furtherance of the Olympus fraud was cleared through COMMERZ NEW YORK.

40. COMMERZ NEW YORK failed to file a SAR in the United States concerning Olympus or any of the Olympus-related entities until November 2013 – more than two years after the Olympus accounting fraud was revealed.

COMMERZ NEW YORK's Compliance Deficiencies

41. The same individual served as COMMERZ NEW YORK's BSA Officer continuously from approximately 2003 until early 2014. Over those years, she raised concerns about AML compliance, both to her superiors at COMMERZ NEW YORK, and with COMMERZ Frankfurt.

42. Under the BSA, a financial institution is required to detect and report suspicious activity. This is accomplished, in part, through conducting due diligence, and enhanced due diligence where appropriate, of the correspondent relationship – which COMMERZ NEW YORK failed to do – and by sending requests for further information to the correspondent bank when potentially suspicious transactions are detected.

43. COMMERZ NEW YORK frequently had difficulties getting responses to requests for information that were generated in connection with automated transaction monitoring "alerts." Because requests for information went unanswered for as much as eight months without SARs being filed, alerts were often closed without any response to the pending request. As a result of these deficiencies, COMMERZ NEW YORK cleared numerous AML "alerts" based on its own perfunctory internet searches and searches of public source databases but without ever receiving responses to its requests for information.

44. On or about June 24, 2010, a COMMERZ NEW YORK-based compliance officer who had primary responsibility for automated transaction monitoring wrote in an e-mail to the BSA Officer and the Head of Compliance in New York (who had previously served as the Head of Compliance in Asia) that "we currently have 90 alerts a day," with "808 alerts outstanding," which "could lead to a possible back log." He continued, "I also wanted to make you aware that we have currently over 130 Frankfurt RFIs [i.e., requests for information] outstanding," noting "a decrease in response to the RFIs" from Frankfurt. The following day, the Head of Compliance in New York forwarded the e-mail to Commerz's Global Head of Compliance, adding that "things are not getting better with regards to th[ose] findings. (see below). I will forward you the DRAFT memo on potential revision of staffing needs." Although the Global Head of Compliance thereafter instituted new procedures designed to increase the speed of responses to RFIs from New York, problems persisted with the timely flow of information from business units outside the U.S. to compliance officers in New York.

45. At all times relevant to this Information, COMMERZ and COMMERZ NEW YORK failed to conduct adequate due diligence or to obtain "know your customer" information with respect to correspondent bank accounts for COMMERZ's own foreign branches and

affiliates. These systemic deficiencies reflected a failure to maintain adequate policies, procedures, and controls to ensure compliance with the BSA and regulations prescribed thereunder and to guard against money laundering.

Statutory Allegation

46. From in or about 2008, through in or about 2013, in the Southern District of New York and elsewhere, the defendant

COMMERZBANK AG NEW YORK BRANCH

acting through certain employees located in New York, did willfully violate the Bank Secrecy Act, 31 U.S.C. §§ 5318(h) and 5322, and regulations issued thereunder, that is, 31 C.F.R. § 1022.210 (a) (formerly Section 103.125(a)), by failing to develop, implement and maintain an effective anti-money laundering program. Specifically, defendant COMMERZBANK AG NEW YORK BRANCH, at a minimum, willfully: (a) failed to adequately conduct investigations of transactions that were deemed potentially suspicious or that "alerted" in COMMERZBANK AG NEW YORK BRANCH's automated AML software, instead closing investigations of potentially suspicious transactions based on no or insufficient information received in response to requests for information; (b) failed to report suspicious activity including wire transfers through COMMERZBANK AG NEW YORK BRANCH that ultimately furthered the Olympus accounting fraud; and (c) failed to adequately monitor billions of dollars in correspondent banking transactions, including by failing to conduct any due diligence on COMMERZBANK branches and inadequate due diligence on COMMERZBANK affiliates.

(Title 31, United States Code, Sections 5318(h) and 5322(b) & (c); and
Title 31, Code of Federal Regulations, Section 1020.210).

COUNT THREE

(Violation of the Bank Secrecy Act:
Failure to File a Suspicious Activity Report)

The United States further charges:

47. The allegations contained in paragraphs 1 through 20, 22, 24-27, and 29-45 above are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

48. From in or about 2008 through in or about 2013, in the Southern District of New York and elsewhere, the defendant

COMMERZBANK AG NEW YORK BRANCH

acting through certain employees located in New York, did willfully fail to report suspicious transactions relevant to a possible violation of law or regulations, as required by the Secretary of the Treasury, to wit, COMMERZBANK AG NEW YORK BRANCH the defendant, failed to file Suspicious Activity Reports in the United States with respect to correspondent banking transactions.

(Title 31, United States Code, Sections 5318(g) and 5322(b) & (c); and
Title 31, Code of Federal Regulations, Section 1020.320).

COUNT FOUR

(Violation of the Bank Secrecy Act:
Failure to Conduct Due Diligence on Correspondent Banking Accounts)

The United States further charges:

49. The allegations contained in paragraphs 1 through 20, 22, 24-27, and 29¬45 above are hereby repeated, realleged and incorporated by reference as if fully set forth herein.

50. From in or about 2008, through in or about 2013, in the Southern District of New York and elsewhere, the defendant

COMMERZBANK AG NEW YORK BRANCH

acting through certain employees located in New York, did willfully fail to conduct due diligence on correspondent bank accounts for non-United States persons, to wit, COMMERZBANK AG NEW YORK BRANCH failed to obtain adequate due diligence or "know your customer" information on foreign institutions owned by or affiliated with COMMERZBANK AG for which COMMERZBANK AG NEW YORK BRANCH maintained correspondent accounts, information that if collected and maintained would have reasonably allowed for the detection and reporting of instances of money laundering and other suspicious activity through those accounts.

(Title 31, United States Code, Sections 5318(i) and 5322(d); and
Title 31, Code of Federal Regulations, Section 1010.610).

FORFEITURE ALLEGATION

51. Upon conviction of the offense alleged in Count One, COMMERZ BANK AG shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to this offense, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). The United States will seek entry of a forfeiture money judgment in respect of Count One in the amount of at least $263,000,000.

52. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

COMMERZBANK AG shall forfeit to the United States any other property of COMMERZBANK AG, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28 United Sates Code, Section 2461(c), and Title 21, United States Code, Section 853(p))

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
FOR THE DISTRICT OF COLUMBIA

3-11-15
DATE

Matt Graves, D.C. Bar No. 481052
Maia Miller, VA Bar No. 73221
Assistant United States Attorneys
555 Fourth Street, N.W.
Washington, D.C. 20530
(202) 252-7762 (Graves)
(202) 252-6737 (Miller)
matthew.graves@usdoj.gov
maia.miller@usdoj.gov

LESLIE CALDWELL
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

M. KENDALL DAY
ACTING CHIEF, ASSET FORFEITURE
AND MONEY LAUNDERING SECTION

3-11-15
DATE

Sarah Devlin
Trial Attorney
Asset Forfeiture and Money Laundering
Section

PREET BHARARA
UNITED STATES ATTORNEY
FOR THE SOUTHERN DISTRICT OF NEW
YORK

3-11-15
DATE

Bonnie Jonas
Assistant United States Attorney