

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

COMMERZBANK AG, and
COMMERZBANK AG NEW YORK
BRANCH,

Defendants.

CRIMINAL NO. _____

VIOLATIONS: 18 U.S.C. § 371
(Conspiracy to Violate IEEPA);
31 U.S.C. §§ 5318(g), 5318(h),
5318(i), and 5322(b)
(Violations of the BSA)

FORFEITURE: 21 U.S.C. § 853(p); 18
U.S.C. § 981(a)(1)(C); and 28 U.S.C.
§ 2461(e)

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 IFFPA.

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(j)(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 Depositary 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 (b) 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 States Code, Section 2461(c), and Title 21, United States Code,
Section 853(p))

3-11-15

DATE

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

Matt Graves

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

DATE

Sarah Devlin
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

Bonnie Jonas
Assistant United States Attorney

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA : CRIMINAL NO. _____
 :
 v. :
 :
 :
 COMMERZBANK AG, and :
 COMMERZBANK AG NEW YORK :
 BRANCH :
 :
 Defendants. :
 :

DEFERRED PROSECUTION AGREEMENT

Defendant Commerzbank AG and Commerzbank AG New York Branch (collectively, the "Company"), by its undersigned representatives, pursuant to authority granted by the Company's Board of Directors, and the United States Department of Justice, Criminal Division, Asset Forfeiture and Money Laundering Section; the United States Attorney's Office for the District of Columbia; and the United States Attorney's Office for the Southern District of New York (the "Offices"), enter into this deferred prosecution agreement (the "Agreement"), the terms and conditions of which are as follows:

Criminal Information and Acceptance of Responsibility

1. The Company acknowledges and agrees that the Offices will file the attached four-count criminal Information in the United States District Court for the District of Columbia charging the Company with (1) knowingly and willfully conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), in violation of Title 18, United States Code, Section 371, and Title 50, United States Code, Sections 1701-1705, and the regulations issued thereunder; and (2) willfully violating various provisions of the Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the Bank Secrecy Act, or "BSA"), including (a) failure to maintain an effective anti-money laundering ("AML") program,

in violation of Title 31, United States Code, Sections 5318(h) and 5322(b) & (c); (b) failure to file suspicious activity reports, in violation of Title 31, United States Code, Sections 5318(g) and 5322(b) & (c); and (c) failure to establish due diligence for foreign correspondent accounts, in violation of Title 31, United States Code, Sections 5318(i) and 5322(d). In so doing, the Company: (a) knowingly waives its right to indictment on these charges, as well as all rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Title 18, United States Code, Section 3161, and Federal Rule of Criminal Procedure 48(b); and (b) knowingly waives, for purposes of this Agreement and any charges by the United States arising out of the conduct described in the attached Statements of Fact, any objection with respect to venue and consents to the filing of the Information, as provided under the terms of this Agreement, in the United States District Court for the District of Columbia.

2. The Company admits, accepts, and acknowledges that it is responsible under United States law for the acts of its officers, directors, employees, and agents as charged in the Information, and as set forth in the Statements of Fact attached hereto as Attachments A and B and incorporated by reference into this Agreement, and that the allegations described in the Information and the facts described in Attachments A and B are true and accurate. Should the Offices pursue the prosecution that is deferred by this Agreement, the Company stipulates to the admissibility of the Statements of Fact in any proceeding, including any trial, guilty plea, or sentencing proceeding, and will not contradict anything in the Statements of Fact at any such proceeding.

Term of the Agreement

3. This Agreement is effective for a period beginning on the date on which the Information is filed and ending three (3) years from that date (the "Term"). The Company agrees, however, that, in the event the Offices determine, in their sole discretion, that the

Company has knowingly violated any provision of this Agreement, an extension or extensions of the term of the Agreement may be imposed by the Offices, in their sole discretion, for up to a total additional time period of one year, without prejudice to the Offices' right to proceed as provided in Paragraphs 18 through 22 below. Any extension of the Agreement extends all terms of this Agreement, including the terms of the reporting requirement in Paragraph 13, for an equivalent period. Conversely, in the event the Offices find, in their sole discretion, that there exists a change in circumstances sufficient to eliminate the need for the reporting requirement in Paragraph 13, and that the other provisions of this Agreement have been satisfied, the Term of the Agreement may be terminated early.

Relevant Considerations

4. The Offices enter into this Agreement based on the individual facts and circumstances presented by this case and the Company. Among the factors considered were the following: (a) the Company's willingness to acknowledge and accept responsibility for the actions of its officers, directors, employees, and agents as charged in the Information and as set forth in the Statements of Fact; (b) the Company's remedial actions taken to date; (c) the Company's agreement to continue to enhance its sanctions and BSA/AML compliance programs; (d) the Company's agreement to continue to cooperate with the Offices in any ongoing investigation of the conduct of the Company and its current or former officers, directors, employees, and agents as provided in Paragraph 5 below; (e) the Company's willingness to settle any and all civil and criminal claims currently held by the Offices for any act within the scope of the Statements of Fact; and (f) the Company's cooperation with the Offices, including voluntarily making U.S. and foreign employees available for interviews, and collecting, analyzing, and organizing voluminous evidence and information for the Offices.

Future Cooperation and Disclosure Requirements

5 The Company shall cooperate fully with the Offices in any and all matters relating to the conduct described in this Agreement and Attachments A and B and other conduct under investigation by the Offices, at any time during the Term of this Agreement, subject to applicable laws and regulations, until the date upon which all investigations and prosecutions arising out of such conduct are concluded, whether or not those investigations and prosecutions are concluded within the term specified in Paragraph 3. At the request of the Offices, the Company shall also cooperate fully with other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of the Company, or its affiliates, or any of its present or former officers, directors, employees, agents, and consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and Attachments A and B and other conduct under investigation by the Offices or any other component of the Department of Justice at any time during the Term of this Agreement, subject to applicable laws and regulations. The Company agrees that its cooperation pursuant to this paragraph shall include, but not be limited to, the following:

a. The Company shall truthfully disclose all factual information not protected by a valid claim of attorney-client privilege or work product doctrine with respect to its activities, those of its affiliates, and those of its present and former directors, officers, employees, agents, and consultants, including any evidence or allegations and internal or external investigations, related to investigations by the Offices known to the Company or about which the Offices may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Company to provide to the Offices, upon request, any document, record or other tangible evidence about which the Offices may inquire of the Company.

b. Upon request of the Offices, the Company shall designate knowledgeable employees, agents, or attorneys to provide to the Offices the information and materials described in Paragraph 5(a) above on behalf of the Company. It is further understood that the Company must at all times provide complete, truthful, and accurate information.

c. The Company shall, at its cost, use its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, agents and consultants of the Company. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation under this Paragraph shall include identification of witnesses who, to the knowledge of the Company, may have material information regarding the matters under investigation.

d. Upon request from the Offices, the Company shall use its good faith efforts to identify additional witnesses who, to the Company's knowledge, may have material information concerning this investigation, and notify the Offices.

e. With respect to any information, testimony, documents, records, or other tangible evidence provided to the Offices pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities and those of a foreign government of such materials as the Offices, in their sole discretion, shall deem appropriate.

f. The Company shall provide information, materials, and testimony as necessary or requested to identify or to establish the original location, authenticity, or other basis for admission into evidence of documents or physical evidence in any criminal or judicial proceeding.

6. In addition to the obligations in Paragraph 5, during the Term of the Agreement, should the Company learn of credible evidence or allegations of any violation of United States federal law, including any criminal conduct by the Company or any of its employees acting within the scope of their employment, the Company shall promptly report such evidence or allegations to the Offices. The Company shall likewise bring to the Offices' attention any administrative, regulatory, civil, or criminal proceeding or investigation of the Company relating to the BSA or the anti-money laundering laws of any other jurisdiction. Nothing in this Agreement shall be construed to require the Company to produce any documents, records or tangible evidence that are protected by the attorney-client privilege, work product doctrine, or subject to the rules and regulations of the regulators regarding the disclosure of confidential supervisory information, or to take any steps in violation of German or other applicable law and legal principles.

Payment of Monetary Penalty

7. The Offices and the Company agree that, based on the factors set forth in 18 U.S.C. § 3572(a), and 18 U.S.C. § 3571(d), a fine of \$79 million is an appropriate fine in this case. The Company agrees to pay a fine in the amount of \$79 million to the United States Treasury within five (5) business days of the date on which this Agreement is signed. The fine amount represents twice the value of the transactions identified in Paragraph 65 of Attachment A. The Company and the Offices agree that this fine is appropriate given the facts and circumstances of this case, including the nature and seriousness of the Company's conduct. The \$79 million fine is final and shall not be refunded. Furthermore, nothing in this Agreement shall be deemed an agreement by the Offices that \$79 million is the maximum fine that may be imposed in any future prosecution, and the Offices are not precluded from arguing in any future prosecution that the Court should impose a higher fine, although the Offices agree that under

those circumstances, they will recommend to the Court that any amount paid under this Agreement should be offset against any fine the Court imposes as part of a future judgment. The Company agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any federal, state, local, or foreign tax for any fine paid pursuant to this Agreement. The Company shall pay the fine plus any associated transfer fees within five (5) business days of the date on which this Agreement is signed, pursuant to payment instructions provided by the Offices in their sole discretion. The Company releases any and all claims it may have to such funds, and further certifies that it passes clean title to these funds, which are not the subject of any lien, security agreement, or other encumbrance. Transferring encumbered funds or failing to pass clean title to the funds in any way will be considered a breach of this agreement. The Company shall indemnify the government for any costs it incurs associated with the passing of clean title to the funds.

Forfeiture

8. As a result of the conduct described in the Information and Attachments A and B, the Company agrees to make a total payment in the amount of \$563 million (the "Forfeiture Amount") pursuant to this Agreement. The Forfeiture Amount is comprised of a payment of \$263 million on account of the conduct described in Attachment A (the "Sanctions Forfeiture Amount"), and \$300 million on account of the conduct described in Attachment B (the "BSA/AML Forfeiture Amount"). The Government intends to distribute the BSA/AML Forfeiture Amount to victims of the fraud at the Olympus Corporation, consistent with the applicable Department of Justice regulations. See 21 U.S.C. § 853(i)(1) and 28 C.F.R. Part 9.

a. The Company agrees that the facts contained in the Information and Attachment A establish that the Sanctions Forfeiture Amount is subject to civil forfeiture to the United States and that this Agreement, the Information, and Attachment A shall be attached and

incorporated into a civil forfeiture complaint (the "Sanctions Civil Forfeiture Complaint"), a copy of which is attached hereto as Attachment D, that will be filed against the Sanctions Forfeiture Amount in the United States District Court for the District of Columbia. The Company further agrees that the funds used to pay the Sanctions Forfeiture Amount were funds involved in transactions which promoted the carrying on of the conspiracy to violate IEEPA. The Company agrees that there is a substantial connection between the funds used to pay the Sanctions Forfeiture Amount and the offense alleged in the Sanctions Civil Forfeiture Complaint.

b. The Company agrees that the facts contained in the Information and Attachment B establish that the BSA/AML Forfeiture Amount is subject to civil forfeiture to the United States, and that this Agreement, the Information, and Attachment B shall be attached and incorporated into a civil forfeiture complaint (the "BSA/AML Civil Forfeiture Complaint"), a copy of which is attached hereto as Attachment E, that will be filed against the BSA/AML Forfeiture Amount in the United States District Court for the Southern District of New York.

c. By this Agreement, the Company expressly waives all constitutional and statutory challenges in any manner to any forfeiture carried out in accordance with this Agreement on any grounds, including that the forfeiture constitutes an excessive fine or punishment. The Company also waives service of the Sanctions Civil Forfeiture Complaint and the BSA/AML Civil Forfeiture Complaint, and *in rem* jurisdiction as to the Sanctions Forfeiture Amount and the BSA/AML Forfeiture Amount. The Company agrees to sign any documents, including a stipulation as to the involvement of the Sanctions Forfeiture Amount in the transactions in violation of IEEPA, necessary for the Government to complete the forfeiture of

the funds used to pay the Forfeiture Amount. The Company further agrees to the entry of Final Orders of Forfeiture against the Forfeiture Amount.

d. Upon Court approval of this Agreement, the Company shall release any and all claims it may have to the Forfeiture Amount and execute such documents as necessary to accomplish the forfeiture of the funds. The Company agrees that it will not file a claim with any Court or otherwise contest the civil forfeiture of the Forfeiture Amount and will not assist a third party in asserting any claim to the Forfeiture Amount. The Company certifies that the funds used to pay the Forfeiture Amount are not the subject of any lien, security agreement, or other encumbrance. Transferring encumbered funds or failing to pass clean title to these funds in any way will be considered a breach of this agreement.

e. The Company agrees that the Forfeiture Amount shall be treated as a penalty paid to the United States government for all purposes, including tax purposes. The Company agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any federal, state, local, or foreign tax for any fine or forfeiture paid pursuant to this Agreement.

f. The Company shall transfer the entire Forfeiture Amount of \$563 million less the credit set forth in paragraph 8(h)—totaling \$392 million—within five (5) business days after executing this Agreement (or as otherwise directed by the Offices following such period) and shall pay any associated transfer fees. Such payment shall be made pursuant to wire instructions provided by the Offices. If the Company fails to timely make the payment required under this paragraph, interest (at the rate specified by 28 U.S.C. § 1961) shall accrue on the unpaid balance through the date of payment, unless the Offices, in their sole discretion, chooses to reinstate prosecution pursuant to Paragraphs 18-22, below.

g. The Forfeiture Amount paid is final and shall not be refunded should the Government later determine that the Company has breached this Agreement and commences a prosecution against the Company. In the event of a breach of this Agreement and subsequent prosecution, the Government may pursue additional civil and criminal forfeiture in excess of the Forfeiture Amount. The Government agrees that in the event of a subsequent breach and prosecution, it will recommend to the Court that the amounts paid pursuant to this Agreement be offset against whatever forfeiture the Court shall impose as part of its judgment. The Company understands that such a recommendation will not be binding on the Court.

h. The Offices agree that payments by the Company in connection with its concurrent settlement of the related criminal action brought by the New York County District Attorney's Office, totaling \$171 million, shall be credited against the Sanctions Forfeiture Amount. The Company agrees to make the payment of \$171 million to an account designated by the New York County District Attorney's Office.

Conditional Release from Liability

9. Subject to Paragraphs 18 through 22, the Offices agree, except as provided herein, that they will not bring any criminal or civil case against the Company or any of its subsidiaries, affiliates, successors or assigns, relating to: any of the conduct described in the Statements of Fact, attached hereto as Attachments A and B, or the criminal Information filed pursuant to this Agreement. The Offices, however, may use any information related to the conduct described in the attached Statements of Facts against the Company: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code.

a. This Agreement does not provide any protection against prosecution for any future conduct by the Company.

b. This Agreement does not provide any protection against prosecution for conduct that is not explicitly referenced in Attachments A and B, the criminal Information filed pursuant to this Agreement, or that was not disclosed by the Company or its subsidiaries to the Offices prior to the date on which this Agreement was signed.

c. This Agreement does not provide any protection against prosecution of any present or former officer, director, employee, shareholder, agent, consultant, contractor, or subcontractor of the Company for any violations committed by them.

d. Notwithstanding the foregoing, all civil claims of the United States related to the allegations in the Amended Complaint filed on or about August 17, 2014 in United States ex rel. [Under Seal] v. [Under Seal], No. 13 Civ. 8095 (S.D.N.Y.), are expressly reserved and excluded from any release of liability, nothing herein shall be construed to release, impair or otherwise affect any such claims of the United States, and no amount paid by the Company or its subsidiaries in connection with this agreement may be used to offset any recovery of the United States pursuant to any such claims.

Corporate Compliance Program

10. The Company represents that it has implemented and will continue to implement a compliance and ethics program designed to prevent and detect violations of Title 50, United States Code, Section 1705, and the regulations issued thereunder, throughout its operations, including those of its affiliates, agents, and joint ventures the Company can control, whose operations include managing client accounts for clients subject to Office of Foreign Asset Control ("OFAC") sanctions, processing payments denominated in United States Dollars, and directly or indirectly supervising such operations. The Company has further represented that it

has implemented and will continue to implement a compliance and ethics program designed to ensure compliance with the BSA, including implementing an effective anti-money laundering compliance program, adequate customer due diligence for correspondent accounts, and appropriate detection and reporting of suspicious activity.

11. In order to address any deficiencies in its sanctions compliance programs, the Company represents that it shall:

a. Continue to apply the OFAC sanctions list to United States Dollar (“USD”) transactions, the acceptance of customers, and all USD cross-border Society for Worldwide Interbank Financial Telecommunications (“SWIFT”) incoming and outgoing messages involving payment instructions or electronic transfer of funds;

b. Not knowingly undertake any USD cross-border electronic funds transfer or any other USD transaction that is prohibited by U.S. law or OFAC regulations concerning Iran, North Korea, the Sudan (except for those regions and activities exempted from the United States embargo by Executive Order No. 13412), Syria, Cuba, or Burma;

c. Continue to complete Financial Economic Crime sanctions training, covering U.S., U.N., and E.U. sanctions and trade control laws for all employees (1) involved in the processing or investigation of USD payments and all employees and officers who directly or indirectly are supervising these employees, (2) involved in execution of USD denominated securities trading orders and all employees and officers who directly or indirectly are supervising these employees; and (3) involved in transactions or business activities involving any nation or entity subject to U.S., E.U., or U.N. sanctions, including the execution of cross border payments;

d. Continue to apply its written policy requiring the use of SWIFT Message Type ("MT") MT1 202COV bank-to-bank payment message where appropriate under SWIFT Guidelines, and by May 30, 2015, certify continuing application of that policy;

e. Continue to apply and implement compliance procedures and training designed to ensure that the Company's compliance officer in charge of sanctions is made aware in a timely manner of any known requests or attempts by any entity (including, but not limited to, the Company's customers, financial institutions, companies, organizations, groups, or persons) to withhold or alter its name or other identifying information where the request or attempt appears to be related to circumventing or evading U.S. sanctions laws. The Company's Head of Compliance, or his or her designee, shall report to the Offices in a timely manner, the name and contact information, if available to the Company, of any entity that makes such a request;

f. Maintain the electronic database of SWIFT Message Transfer payment messages and all documents and materials produced by the Company to the United States as part of this investigation relating to USD payments processed during the period from 2002 through 2008 in electronic format during the period of this Agreement, including any extensions;

g. Abide by any and all requirements of the Settlement Agreement, insert date, by and between OFAC and the Company regarding remedial measures or other required actions related to this matter;

h. Abide by any and all requirements of the Cease and Desist Order, insert date, by and between the Board of Governors of the Federal Reserve System and the Company regarding measures or other required actions related to this matter;

i. Abide by and all requirements of the Settlement Agreement, insert date, by and between the New York Department of Financial Services and the Company regarding remedial measures or other required actions related to this matter;

j. The Company shall share with the Offices any reports, disclosures, or information that the Company, by terms of these settlement agreements, and the Cease-and-Desist order, is required to provide to OFAC, the Federal Reserve, and the Department of Financial Services. The Company further agrees that any compliance consultant or monitor imposed by the Federal Reserve or the New York State Department of Financial Services ("DFS") shall, at the Company's own expense, submit to the Offices any report that it submits to the Federal Reserve or DFS.

12. With respect to BSA/AML compliance, the Company shall continue its ongoing effort to implement and maintain an effective BSA/AML compliance program in accordance with the requirements of the BSA and the directives and orders of any United States regulator of the Company or its affiliates, including without limitation the Federal Reserve Board, as set forth in its Cease and Desist Order, dated October 16, 2013, and its Written Agreement with the Company, dated June 8, 2012 (the "Consent Orders").

Corporate Compliance Reporting

13. The Company agrees that it will report to the Offices every 90 days during the term of the Agreement regarding remediation and implementation of the compliance measures described in Paragraphs 10-12. Such reports must include specific and detailed accounts of the Company's sanctions and BSA/AML compliance improvements, and must identify any violations of the BSA that have come to the attention of the Company's legal and compliance personnel during the reporting period. At the end of the term of the Agreement, the Company's

Chief Executive Officer must certify via his or her signature that the Company's sanctions and BSA/AML compliance improvements have been completed.

14. The Company shall notify the Offices of any criminal, civil, administrative or regulatory investigation, inquiry, or action, of the Company or its current directors, officers, employees, consultants, representatives, and agents related to the Company's compliance with United States sanctions or anti-money laundering laws, to the extent permitted by the agency conducting the investigation or action and applicable law. It is understood that the Company shall promptly notify the Offices of (a) any deficiencies, failing, or matters requiring attention with respect to the Company's BSA/AML compliance program identified by any United States regulatory authority within 10 business days of any such regulatory notice; and (b) any steps taken or planned to be taken by the Company to address the identified deficiency, failing, or matter requiring attention. The Offices may, in their sole discretion, direct the Company to provide other reports about its BSA/AML compliance program as warranted.

15. For the duration of the Agreement, the Offices, as they deem necessary and upon request to the Company, shall: (a) be provided by the Company with access to any and all non-privileged books, records, accounts, correspondence, files, and any and all other documents or electronic records, including e-mails, of the Company and its representatives, agents, affiliates, and employees, relating to any matters described or identified in the reports, without regard to the location of such materials, and (b) have the right to interview any officer, employee, agent, consultant, or representative of the Company concerning any non-privileged matter described or identified in the reports, without regard to the location of such person. To the extent the provisions of this paragraph relate to information or attendance of personnel located outside of the United States, the parties to this Agreement acknowledge that the request,

provision, or use of such information, or attendance of personnel, is subject to applicable laws and legal principles in the relevant jurisdiction.

Deferred Prosecution

16. In consideration of: (a) the past and future cooperation of the Company described in Paragraphs 5 and 6 above; (b) the Company's payment of a fine of \$79 million and forfeiture of \$563 million; and (c) the Company's implementation and maintenance of remedial measures as described in Paragraphs 10-12 above, the Offices agree that any prosecution of the Company for the conduct set forth in the attached Statements of Fact, the criminal Information filed pursuant to this Agreement, and for the conduct that the Company or its subsidiaries disclosed to the Offices prior to the signing of this Agreement, be and hereby is deferred for the Term of this Agreement.

17. The Offices further agree that if the Company fully complies with all of its obligations under this Agreement, the Offices will not continue the criminal prosecution against the Company described in Paragraph 1 and, at the conclusion of the Term, this Agreement shall expire. Within thirty (30) days of the Agreement's expiration, the Offices shall seek dismissal with prejudice of the criminal Information filed against the Company described in Paragraph 1, and agrees not to file charges in the future against the Company based on the conduct described in this Agreement and in Attachments A and B.

Breach of the Agreement

18. If, during the Term of this Agreement, the Company (a) commits any felony under United States federal law; (b) provides in connection with this Agreement deliberately false, incomplete, or misleading information; (c) fails to cooperate as set forth in Paragraphs 5 and 6 of this Agreement; (d) fails to implement a compliance program as set forth in Paragraphs 10-12 of this Agreement; or (e) otherwise fails specifically to perform or to fulfill

completely each of the Company's obligations under the Agreement, the Company shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited to, the charges in the Information described in Paragraph 1, which may be pursued by the Offices in the United States District Court for the District of Columbia, the United States District Court for the Southern District of New York, or any other appropriate venue. Determination of whether the Company has breached the Agreement and whether to pursue prosecution of the Company shall be in the Offices' sole discretion. Any such prosecution may be premised on information provided by the Company. Any such prosecution relating to the conduct described in the attached Statements of Fact or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Company, notwithstanding the expiration of the statute of limitations, between the signing of this Agreement and the expiration of the Term plus one year. Thus, by signing this Agreement, the Company agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term plus one year.

19. In the event the Offices determine that the Company has breached this Agreement, the Offices agree to provide the Company with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty (30) days of receipt of such notice, the Company shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of such breach, as well as the actions the Company has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to pursue prosecution of the Company.

20. In the event that the Offices determine that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Offices or to the Court, including the attached Statements of Fact, and any testimony given by the Company before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against the Company; and (b) the Company shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the Company prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director, officer or employee, or any person acting on behalf of, or at the direction of, the Company, will be imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Offices.

21. The Company acknowledges that the Offices have made no representations, assurances, or promises concerning what sentence may be imposed by the Court if the Company breaches this Agreement and this matter proceeds to judgment. The Company further acknowledges that any such sentence is solely within the discretion of the Court and that nothing in this Agreement binds or restricts the Court in the exercise of such discretion.

22. No later than 90 days prior to the expiration of the period of deferred prosecution specified in this Agreement, the Company, by the management board member who oversees compliance, will certify, on behalf of the Company, to the Offices that the Company has met its disclosure obligations pursuant to Paragraph 6 of this Agreement. Such certification will be

deemed a material statement and representation by the Company to the executive branch of the United States for purposes of 18 U.S.C. § 1001, and it will be deemed to have been made in the judicial district in which this Agreement is filed.

Sale or Merger of Company

23. Except as may otherwise be agreed by the parties hereto in connection with a particular transaction, the Company agrees that in the event it sells, merges, or transfers all or substantially all of its business operations as they exist as of the date of this Agreement, whether such sale is structured as a sale, asset sale, merger, or transfer, it shall include in any contract for sale, merger, or transfer a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement.

Public Filing

24. The Company and the Offices agree that, upon submission of this Agreement (including the Statements of Fact and other attachments hereto) to the Court, the Agreement (and its attachments) shall be filed publicly in the United States District Court for the District of Columbia.

Public Statements by Company

25. The Company expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents, or any other person authorized to speak for the Company make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Company set forth above or the facts described in the attached Statements of Fact. Any such contradictory statement shall, subject to cure rights of the Company described below, constitute a breach of this Agreement, and the Company thereafter shall be subject to prosecution as set forth in Paragraphs 18 through 22 of this Agreement. The decision whether any public statement by any such person contradicting a fact contained in the Statements of Fact

will be imputed to the Company for the purpose of determining whether it has breached this Agreement shall be at the sole discretion of the Offices. If the Offices determine that a public statement by any such person contradicts in whole or in part a statement contained in the Statements of Fact, the Offices shall so notify the Company, and the Company may avoid a breach of this Agreement by publicly repudiating such statement(s) within five (5) business days after notification. The Company shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Statements of Fact provided that such defenses and claims do not contradict, in whole or in part, a statement contained in the Statements of Fact. This Paragraph does not apply to any statement made by any present or former officer, director, employee, or agent of the Company in the course of any criminal, regulatory, or civil case initiated against such individual, unless such individual is speaking on behalf of the Company.

26. The Company agrees that if it issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult with the Offices to determine (a) whether the text of the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Company; and (b) whether the Offices have any objection to the release. The Company further agrees that upon learning of any plans by a subsidiary or affiliate to issue a press release or hold a press conference in connection with the Agreement, it will promptly consult with the Offices as provided in the prior sentence.

27. The Offices agree, if requested to do so, to bring to the attention of law enforcement and regulatory authorities the facts and circumstances relating to the nature of the conduct underlying this Agreement, including the nature and quality of the Company's cooperation and remediation. By agreeing to provide this information to such authorities, the

Offices are not agreeing to advocate on behalf of the Company, but rather are agreeing to provide facts to be evaluated independently by such authorities.

Limitations on Binding Effect of Agreement

28. This Agreement is binding on the Company and the Offices but specifically does not bind any other component of the Department of Justice, other federal agencies, or any state, local or foreign law enforcement or regulatory agencies, or any other authorities, although the Offices will bring the cooperation of the Company and its compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by the Company. This agreement does not bind any affiliates or subsidiaries of the Company, other than those that are parties to this Agreement, but is binding on the Company itself. To the extent the Company's compliance with this agreement requires it, the Company agrees to ensure that its wholly-owned subsidiaries, and any successors and assigns, comply with the requirements and obligations set forth in this agreement, to the full extent permissible under locally applicable laws and regulations, and the instructions of local regulatory agencies.

Notice

29. Any notice to the Offices under this Agreement shall be given by personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to:

M. Kendall Day
Acting Chief, Asset Forfeiture and Money Laundering Section
Criminal Division
U.S. Department of Justice
1400 New York Ave. NW
Washington, DC 20005

with copies to:

Ronald C. Machen Jr.
United States Attorney for the District of Columbia
555 4th Street NW
Washington, DC 20530

and:

Preet Bharara
United States Attorney for the Southern District of New York
1 Saint Andrew's Plaza
New York, New York 10007

Any notice to the Company under this Agreement shall be given by personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to:

Volker Barth
Divisional Board Member Compliance
Hafenstrasse 51
60261 Frankfurt am Main, Germany

Günter Flügge
General Counsel
Kaiserstrasse 16
60261 Frankfurt am Main, Germany

Armin Barthel
Managing Director - Head of Legal North America
225 Liberty Street
New York, NY 10281

Notice shall be effective upon actual receipt by the Offices or the Company.

Execution in Counterparts

30. This Agreement may be executed in one or more counterparts, each of which shall be considered effective as an original signature. Further, all facsimile and digital images of signatures shall be treated as originals for all purposes.

Complete Agreement


31. This Agreement sets forth all the terms of the agreement between the Company and the Offices. No amendments, modifications or additions to this Agreement shall be valid

unless they are in writing and signed by the Offices, the attorneys for the Company, and a duly authorized representative of the Company.

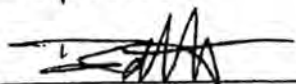
ACCEPTED AND AGREED TO:

FOR COMMERZBANK AG:

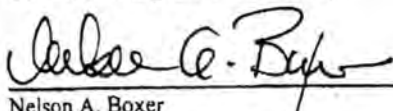
Date: March 14, 2015

By: 
Günter Hugger
Commerzbank AG

Date: March 11, 2015

By: 
Armin Barthel
Commerzbank (New York Branch)

Date: March 11, 2015

By: 
Nelson A. Boxer
Petrillo Klein & Boxer LLP

Date: March 11, 2015

By: 
David Brodsky / Lev Dassin
Cleary Gottlieb Steen & Hamilton LLP

FOR THE DEPARTMENT OF JUSTICE:

Date: 3-11-15

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
FOR THE DISTRICT OF COLUMBIA
BY: Matt Graves
Matt Graves
Maia Miller
Assistant United States Attorneys

Date: 3-11-15

PREET BHARARA
UNITED STATES ATTORNEY
FOR THE SOUTHERN DISTRICT OF
NEW YORK
BY: Bonnie Jonas
Bonnie Jonas
Assistant United States Attorney

Date: 3-11-15

LESLIE CALDWELL
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
M. KENDALL DAY
ACTING CHIEF, ASSET FORFEITURE
AND MONEY LAUNDERING SECTION
BY: Sarah Devlin
Sarah Devlin
Trial Attorney
Asset Forfeiture and Money
Laundering Section

ATTACHMENT A

[Sanctions Statement of Facts]

ATTACHMENT A – STATEMENT OF FACTS

Introduction

1. This Factual Statement is made pursuant to, and is part of, the Deferred Prosecution Agreement dated 3/11/15, between the Criminal Division of the United States Department of Justice, the United States Attorney's Office for the District of Columbia (collectively, "DOJ") and Commerzbank AG ("Commerz"), and between the New York County District Attorney's Office ("DANY") and Commerz. Commerz hereby agrees and stipulates that the following information is true and accurate. Commerz admits, accepts, and acknowledges that it is responsible for the acts of its officers, directors, employees, and agents as set forth below. Should DOJ or DANY pursue the prosecution that is deferred by this Agreement, Commerz agrees that it will neither contest the admissibility of, nor contradict, this Statement of Facts in any such proceeding. The following facts establish beyond a reasonable doubt the charges set forth in the criminal Information attached to this Agreement, and set forth below in Paragraphs 18 and 19. All conduct discussed in this Factual Statement occurred on or about the dates described.

2. Starting in or around January 2002 and ending in or around December 2008, Commerz violated U.S. and New York State laws by assisting clients—such as Iranian companies—in evading U.S. sanctions. Specifically, Commerz sent payments involving sanctioned entities or entities affiliated with sanctioned countries through the U.S. financial system. Commerz knowingly and willfully concealed from U.S. financial institutions and regulators the sanctioned entities' connection to these transactions and intentionally falsified the business records of these institutions. Consequently, U.S. financial institutions processed transactions that otherwise should have been rejected, blocked, or stopped for investigation.

3. Commerz's criminal conduct included, among other things, (i) sending payments from Frankfurt on behalf of sanctioned clients without reference to the payments' origin; (ii) eliminating payment data that would have revealed the involvement of sanctioned entities; (iii) directing an Iranian client to transfer payments in the name of its subsidiary companies to mask the Iranian client's involvement; (iv) issuing checks to an Iranian client that showed only the Iranian bank's account number and not its name; and (v) using alternative payment methods to mask the involvement of sanctioned entities.

4. By providing these banking services to clients that themselves were subject to U.S. sanctions or clients that were doing business with sanctioned entities, Commerz: (i) prevented detection by U.S. regulatory and law enforcement authorities of financial transactions that violated U.S. sanctions; (ii) prevented U.S. financial institutions from filing required sanctions-related reports with the U.S. government; (iii) caused false information and entries to be recorded in the business records of U.S. financial institutions located in New York, New York; and (iv) caused U.S. financial institutions not to make records that they otherwise would have been required by U.S. law to make.

5. This conduct occurred in various business units within Commerz in locations in Germany.

Bank Background

6. Commerz conducts business in Europe, North America, South America, Asia, Africa, and Australia. Commerz is currently headquartered in Frankfurt, Germany, and has over 1,200 branches in Germany alone. Commerz is represented outside Germany by 23 foreign branches, 35 representative offices—including a representative office in Tehran, Iran, from the late 1970s through the relevant period—and 7 subsidiaries, spread across more than 50 countries.

Commerz is listed on exchanges in Germany, London, and Switzerland, and its shares can be purchased in the United States through American Depository Receipts.

7. Since 1967 Commerz has had a license issued by the state of New York to operate as a foreign bank branch in New York, New York. The Branch provides U.S. Dollar ("USD") clearing for international wire payments and provides banking services to German companies, subsidiaries of German companies located in the United States, and U.S. companies.

Applicable Law

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 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 prohibited, 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 included 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"),¹ 31 C.F.R. Part 560, implementing the sanctions imposed by the Executive Orders.

12. With the exception of certain exempt transactions, the ITRs prohibited, 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 the United States Department of the Treasury, Office of Foreign Assets Control ("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 attempt to evade or avoid the restrictions imposed under the ITRs. The ITRs were in effect at all times relevant to the conduct described below.

¹ Effective October 22, 2012, the Department of the Treasury renamed and reissued the ITR as the Iranian Transactions and Sanctions Regulations.

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 entity had direct contact with the Iranian bank or customer and were otherwise permissible (e.g., the transactions were not on behalf of an Specially Designated National (“SDN”)).²

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

² OFAC publishes an 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.

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 prohibited 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.

17. 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.

DOJ Charge

18. DOJ has alleged, and Commerz accepts, that its conduct, as described herein, violated Title 18, United States Code, Section 371, because Commerz conspired to violate IEEPA, which makes it a crime to willfully attempt to commit, conspire to commit, or aid and

abet in the commission of any violation of the regulations prohibiting the export of services from the United States to Iran, Sudan, and SDNs.

DANY Charge

19. DANY has alleged, and Commerz accepts, that its conduct, as described herein, violated New York State Penal Law Sections 175.05 and 175.10, which make it a crime to, “with intent to defraud, . . . 1. [m]ake[] or cause[] a false entry in the business records of an enterprise [(defined as any company or corporation)] . . . or 4. [p]revent[] the making of a true entry or cause[] the omission thereof in the business records of an enterprise.” It is a felony under Section 175.10 of the New York State Penal Law if a violation under Section 175.05 is committed and the person or entity’s “intent to defraud includes an intent to commit another crime or to aid or conceal the commission thereof.”

International Customer Payments at Commerz During the Relevant Period

20. Commerz is a member of the Society for Worldwide Interbank Financial Telecommunications (“SWIFT”) and historically has used the SWIFT system to transmit international payment messages to and from other financial institutions around the world, including its U.S. branch, located in New York, New York. There are a variety of different SWIFT message formats, depending on the type of payment or transfer to be executed. For example, when a corporate or individual customer sends an international wire payment, the de facto standard to execute such a payment is known as an MT 103 SWIFT message, and when a financial institution sends a bank-to-bank credit transfer the de facto standard is known as an MT 202 SWIFT message. The different message types contain different fields of information to be completed by the sending party. During the relevant period, some of these fields were

mandatory—that is, they had to be completed for a payment to be processed—and others were optional.

21. Transactions in USD between two individuals or entities who reside outside the United States and who maintain accounts at different non-U.S. banks typically must transit through the United States through the use of SWIFT messages. This process is typically referred to as “clearing” through U.S. correspondent banks.

22. During the relevant time period, Commerz typically executed and processed international USD payments on behalf of clients in one of two ways. The first method, known as a “serial payment,” was to send a single message, commonly an MT 103, to each financial institution in the transmission chain, identifying the originator and beneficiary of the USD payment. The second method, known as a “cover payment,” involved breaking a payment message into two parts and sending two SWIFT messages in connection with a single payment. In the cover payment method, one message—typically an MT 103—identifying both the originating customer and beneficiary of the payment was sent directly from the customer’s bank (i.e., Foreign Bank A) to the ultimate beneficiary’s bank (i.e., Foreign Bank B) while a second message—typically an MT 202—identifying only the bank originating the cover payment (but not the customer or the beneficiary) accompanied the funds as they transferred through the United States. During the relevant time period, cover payment messages did not require the sending bank to identify the party originating a commercial payment or its ultimate beneficiary, whereas serial payment messages did. As a result, where the cover payment method was employed, the U.S.-based bank did not receive information needed to stop transactions involving sanctioned entities.

Commerz's System for OFAC Compliance During the Relevant Period

23. Financial institutions in the United States are obligated to screen financial transactions, including international wire payments effected through the use of SWIFT messages, to ensure they do not violate U.S. sanctions. Because of the vast volume of wire payments processed by financial institutions in the United States, most institutions employ sophisticated computer software, commonly referred to as filters, to automatically screen all wire payments against a list of sanctioned entities. When the filters detect a possible match to a sanctioned entity, the payment is stopped and held for further manual review. When a financial institution detects a transaction that violates sanctions, the institution must "block" or "reject" the payment—that is, refuse to process or execute the payment and notify OFAC of the attempted transaction. If a party to the payment is an SDN, then the payment must be frozen or "blocked" and the bank must notify OFAC. The sending bank must then demonstrate to OFAC that the payment does not violate sanctions before the funds can be released and the payment processed.

24. During the relevant time period, significant differences existed between Commerz New York's filtering practices and Commerz Frankfurt's filtering practices. Throughout the relevant period, Commerz New York utilized an automated OFAC filter that screened all incoming MT 103 and MT 202 payment messages and, in 2003, Commerz New York significantly upgraded its filtering technologies.

25. Commerz Frankfurt, which processed most international customer payments, lacked an automated sanctions filter for a significant portion of the relevant period. Commerz Frankfurt and other European branches did not begin implementing an automated filtering program until the latter part of 2004, and it was not until 2006 that implementation was completed at all European branches. Moreover, the filter that the European branches

implemented was not as technologically advanced as the one implemented by Commerz New York in 2003. Indeed, Commerz Frankfurt's filter did not receive an upgrade similar to the one Commerz New York received in 2003 until 2011.

26. The differences between Commerz New York's compliance capabilities and the compliance capabilities of the European branches were not limited to the technological differences in the filters they used. There was complete agreement among Commerz New York and Commerz Frankfurt employees interviewed by federal and state investigators that Commerz New York's Compliance personnel had the broadest knowledge of U.S. sanctions of any personnel within the Commerz network. However, Commerz Frankfurt's practice of using cover payments for transactions involving sanctioned countries or entities entirely removed Commerz New York Compliance personnel from the review process, ensuring that cover payments involving sanctioned entities could not be detected or stopped for further review by Commerz New York's filter.

27. As a direct result of this inherently non-transparent payment process, Commerz New York processed approximately \$263 million in transactions in violation of U.S. sanctions. Throughout the relevant time period, certain Commerz Senior Management and Compliance personnel were aware of the policies and procedures that resulted in Commerz processing and sending non-transparent USD payment messages through the United States on behalf of sanctioned clients.

Iran

Background

28. Commerz has a history, dating back to the 1950s, of conducting business on behalf of Iranian banks, corporations, and individuals, as well as non-Iranian clients who engage

in transactions with Iranian entities. Throughout the relevant period, Commerz was sensitive to the potential impact of U.S. sanctions on its Iranian business that cleared through the United States and engaged in various practices to avoid and to evade the impact of U.S. sanctions.

In 2003 Commerz Developed and Memorialized Internal Guidance for Concealing the Iranian Background of USD Payment Messages

29. In light of the concerns about increasing United States scrutiny of Iranian transactions that transited through financial institutions in the United States, various groups within Commerz Frankfurt began preparing and disseminating guidance regarding how European personnel should structure transactions to avoid being delayed, rejected, or blocked in the United States. On April 17, 2003, Commerz finalized a policy entitled, "Routing Instructions Iranian banks for USD payments." This policy admonished employees to "[u]nder no circumstances mention the Iranian background in the cover order." In other words, the Germany-based recipients of this policy were to, under no circumstances, mention the Iranian customer or connection in payment messages sent to the United States. An earlier draft of this policy explained the reason that Iranian links must be removed from payment instructions, warning the reader that "[t]here is a high risk that transactions and cover payments with Iranian Background via USA might be blocked." The target groups for this policy included Commerz Frankfurt, other German branches of the bank, and customer support groups. Neither the final nor draft policies were shared with Commerz New York, though.

30. By concealing these payment details, Commerz Frankfurt prevented Commerz New York and other U.S. financial institutions located in New York and elsewhere in the United States from identifying, reviewing, or stopping transactions that involved sanctioned entities.

In 2003 Commerz Added Iranian Banks As Clients After Other European Banks Ended Their Relationships With the Iranian Banks

31. By the second half of 2003, several of Commerz's European competitors decided to stop processing USD transactions on behalf of Iranian clients and banks due to U.S. Iranian sanctions. Commerz saw this as a business opportunity because several Iranian banks needed to establish new relationships with other financial institutions in order to continue conducting business in USD. The Bank, with the knowledge of Senior Management, took on significant additional USD clearing business on behalf of several Iranian banks. Thus, the issue of clearing Iranian USD payments through the United States took on greater significance.

32. The resulting increase in the volume and significance of Iranian business at Commerz led to the establishment of a centralized process for handling certain Iranian USD payments within Commerz, and the Bank designated one group of employees within the Frankfurt Back Office to manually process those payments. The job of this group was to review payments and amend them if necessary, to ensure that they would not get stopped by OFAC filters when sent to financial institutions in the United States, including Commerz New York. During the relevant period, Commerz had no similar special manual review protocol for payment processing for non-sanctioned countries or entities.

33. In July 2003, a Back Office employee emailed other employees explaining that two state-owned Iranian banks, Bank Melli and Bank Saderat, wanted to begin routing their entire USD clearing business through Commerz. The Back Office employee closed his email by writing, "If for whatever reason CB New York inquires why our turnover has increase [sic] so dramatically **under no circumstances may anyone mention** that there is a connection to the clearing of Iranian banks!!!!!!!!!!!!!!" (emphasis in original). This Back Office employee sent the

email at the direction of the Financial Institutions Group, a large group within Commerz responsible for servicing Commerz's financial institution clients, including the Iranian banks.

34. Commerz employees instructed their Iranian clients about how to help the Bank implement this overwriting policy designed to evade U.S. sanctions or sanctions review in the United States. On September 17, 2003, a Back Office employee sent an email advising a major Iranian Bank that maintained a USD account with Commerz to list "non ref" in the ordering party field in all of its future payment messages. The author of the email had tested Commerz's compliance systems in Frankfurt, and he knew that writing "non ref" would trigger a manual review of the payment, thereby enabling Commerz personnel to ensure that the messages did not contain any Iranian information. And according to one Back Office employee interviewed by federal and state investigators, Commerz personnel explained to employees of Iranian bank clients the kinds of information that could lead to payments being delayed, rejected, or blocked within the United States, and encouraged the Iranian banks to omit this type of information from their payment requests so that Commerz employees would not have to manually remove it.

Senior Management Was Formally Advised of Iranian Payment Modification

35. Senior Management at Commerz knew of the steps taken to evade U.S. sanctions involving Commerz's Iranian clients.

36. In a memo dated October 6, 2003, a Back Office employee informed members of Middle Management that in light of Commerz's increased Iranian business, and a new banking law that came into effect in Germany in July 2003, Section 25b KWG of the Germany Banking Law,³ it was necessary to have clear rules regarding: (i) the "neutralization" of Iranian ordering

³ Section 25b KWG of the German Banking Law required any German financial institution acting as an intermediary bank to include in serial MT103 payment messages the identity of the originating party. The clear purpose of this law was to increase transparency by allowing the recipient of a payment message to know the identity of the entities with whom they were conducting business.

party information by substituting Commerz's bank code, and (ii) the use of cover payments to facilitate Iranian transactions by splitting the messages in two and using Commerz's name in the cover payment messages sent to the United States.

37. Management at Commerz was warned that the Bank's practices for Iranian clients raised "concerns." Specifically, on October 13, 2003, in an email to a member of Commerz's Senior Management, the head of Commerz's Internal Audit division relayed the general concerns expressed by the back office employee on October 6, and advised that Iranian bank names in payment messages transiting through the United States were being "neutralized" and warned that "it raises concerns if we consciously reference the suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the U.S.A." The Senior Executive responded to the Head of Audit that the Senior Executive responsible for Financial Institutions would investigate the issue. When asked by federal and state investigators why he wanted the issue investigated, the Senior Executive held up a copy of the email message he had received from the head of Internal Audit and stated, "this smells."

38. Although members of Middle Management eventually responded to the Senior Executive, they failed to address the problem spotted by the Head of the Audit Division, namely "consciously referenc[ing] the suppression of the ordering party[,] in order to avoid difficulties in the processing of payments with the U.S.A." Rather, in a memo dated November 11, 2003, members of Middle Management informed members of the Board and Senior Management that the April 2003 policy on routing instructions for USD payments from Iranian Banks remained in effect and "in accordance with the [described] U-turn transaction-cover payments[.]" The authors of the November 11, 2003, memo also claimed that overwriting was "not anticipated" with respect to future USD payments "and would contravene [§25b KWG]." Instead, the memo

advocated for the use of cover payments, noting that an advantage of using cover payments for Iranian transactions was that “it can also be avoided that the Iranian banks are mentioned in the . . . cover payments running through the U.S., which is permissible but would raise significant delay” While the authors of the memo expressed their mistaken belief that a policy of using cover payments “takes account of the OFAC regulations” and the Bank’s obligations under German law, they failed to address the original reason the Head of Audit questioned this policy: “consciously referenc[ing] suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the U.S.A.” Senior Management failed to reassert the Head of Audit’s concern. Senior Management also did not take steps to ensure that Middle Management understood that overwriting *could not* occur in light of Middle Management’s representation that overwriting was “not anticipated.” Indeed, Senior Management did not take any steps in response to this memorandum, and overwriting continued.

39. Within a week, Senior Management received a presentation acknowledging that overwriting continued. Specifically, on November 19, 2003, the author of the October 6, 2003, memo circulated a presentation to Senior Management in the Financial Institutions, Audit and Compliance groups that attempted to memorialize the rules Commerz had developed for processing Iranian payments. The presentation discussed a number of different ways SWIFT messages involving Iranian entities could be structured, including: (i) sending a serial MT 103 to all of the banks participating in the transaction, and (ii) using a cover transaction (*i.e.*, splitting a payment into two messages and sending both an MT 103 to the foreign branch of the beneficiary and an MT 202 to the clearing institution in the United States). The presentation noted that for serial MT 103 payments relating to Iran the standard procedure at the Bank had been to manually replace the name of the ordering party with the bank code for Commerz Frankfurt because if the

text were not changed the payments might be blocked due to U.S. sanctions. The presentation warned, however, that altering the identity of the ordering party in an MT 103 might violate a new German law that came into effect in July 2003. Unlike the November 11, 2003, memo, the November 19, 2003, presentation did not represent that overwriting was "not anticipated." Instead, it explicitly stated that MT 103 payments with Iranian backgrounds were "currently being overwritten." Meanwhile, with respect to cover payments, the presentation noted that the Bank's system for generating payment messages automatically replaced the name of the ordering party with the code for Commerz Frankfurt in all MT 202 message sent to the United States. Senior Management failed to provide any type of response to this presentation.

Despite Senior Management Being Put on Notice of Overwriting in October 2003, the Practice Persisted Until July 2004

40. Between October 13, 2003, and March 31, 2004, employees at Commerz adhered to and enforced the bank's Iranian overwriting policies, and the Bank processed transactions in violation of U.S. sanctions.

41. On or about March 31, 2004, the author of the October 6, 2003 memo emailed the members of Senior Management he had emailed on November 19, 2003, noting that they had not provided guidance to the questions he had raised in November 2003 concerning Commerz's overwriting practices with respect to Iranian payments. Despite this reminder, Senior Management failed to take immediate action to address the issue.

42. Between March 31, 2004, and July 23, 2004, employees at Commerz, including an employee within the Frankfurt Compliance Department, adhered to and enforced the Bank's Iranian overwriting policies. The rigor with which the Bank enforced the policy during this period is exemplified by an email from a Back Office employee who wrote, when commenting on the overwriting procedures, "NO EXPERIMENTS PLEASE!!! Have fun with this and

greetings.” (Emphasis in original.) The Bank continued to process transactions in violation of U.S. sanctions.

43. On or about July 23, 2004, Senior Management finally responded to the questions raised starting in October 2003 and provided guidance that the practice of overwriting Iranian MT 103 payment messages should stop. Despite the fact that they were informed that Commerz personnel were using MT 202 messages in processing Iranian payments specifically because this policy “avoided that the Iranian banks are mentioned in the . . . cover payments running through the U.S.,” Senior Management took no steps to investigate whether, as the Head of Audit suggested, such special procedures raised any concerns. Furthermore, neither Senior Management nor any Bank personnel instructed employees at the Iranian banks to cease their practice of omitting information from their payment messages to evade detection by U.S. clearing banks. Senior Management also failed to inform Commerz personnel in New York of the Iranian procedures at Commerz Frankfurt that had been in effect until July 2004, even though it was widely accepted that the Commerz New York employees were far more knowledgeable of U.S. sanctions.

44. Senior Management’s primary response to the concerns first raised in 2003 was to solicit in October 2004 a legal opinion from external counsel regarding OFAC-related transactions and the lack of transparency to the bank’s New York branch from the use of cover payments in those transactions. This opinion was not provided by external counsel until July 2005. In addition, when seeking that opinion from external counsel about the propriety of using cover payments in connection with lawful transactions involving Iran, the Bank failed to disclose that: (i) for over a year, the Bank had a policy of overwriting serial payments; (ii) that the Bank’s procedures advocated using cover payments precisely because cover payments reduced the

likelihood of payments being delayed in the United States; and (iii) that the Head of Audit had expressed reservations about the Bank's use of cover payments specifically because it prevented the U.S. clearing banks from learning of the Iranian background of those payments. Even without all of this information, external counsel—who opined that cover payments could, under certain circumstances, be used in connection with Iranian U-Turn payments—expressed concerns about using cover payments to process Iranian payments in certain contexts. Specifically, external counsel noted that there was “increasing concern among regulators [about the] possible misuse of bank-to-bank transfer mechanisms for what are, in fact, commercial transactions.” External counsel even went so far as, with respect to “wholesale bank-to-bank transfers and netting transactions,” to “advise against the use of [cover payments that contained less robust information about transactions] for purposes of clearing any transaction that may in fact be in respect of a single transaction, or a limited number of transactions, including an identifiable transaction for the benefit of a Blocked Party, as opposed to truly wholesale clearing transactions where many transactions are aggregated and offset.”

Commerz Issued Checks to an Iranian Bank that Intentionally Concealed the Bank's Iranian Identity

45. On June 24, 2004, Commerz employees and employees from Bank Melli, an Iranian bank, devised another method to allow Bank Melli to continue to make USD payments in violation of U.S. sanctions. A member of the Financial Institutions Group reported to a member of Middle Management that he and employees of Bank Melli had agreed that in lieu of sending direct wire payments to beneficiaries in the United States (in violation of U.S. sanctions), Bank Melli would use checks to pay U.S. beneficiaries. The Commerz employee's rationale was that: “The checks do [not] feature stamps or similar, but rather just signatures and display no evidence of an Iranian background and thus can be cleared without any problem.”

46. On July 1, 2004, the Bank provided Bank Melli with 500 checks for a USD account that specifically referenced only Bank Melli's account number, and not its name.

47. Between July 1, 2004, and August 31, 2004, Bank Melli negotiated 108 of these checks for payments into the United States, in violation of IEEPA. These 108 checks had a total value of approximately \$2 million.

Total Commerz Iranian Business During the Relevant Period

48. In total, during the period from January 1, 2002, through December 31, 2007, Commerz processed approximately \$32.7 million in Iranian payments (in addition to the IRISL payments described below) that either terminated in the United States, or otherwise were connected to the United States, in violation of U.S. sanctions, and caused false entries to be made in the business records of financial institutions located in New York, New York.

The Islamic Republic of Iran Shipping Lines

Commerz Established a Relationship with the Islamic Republic of Iran Shipping Lines at a Time When Other European Banks Were Re-evaluating Their Iranian Business

49. In approximately 2002, Commerz Hamburg established a customer relationship with the Islamic Republic of Iran Shipping Lines ("IRISL"), an entity that was designated by OFAC as an SDN on September 10, 2008. By the latter part of 2004, IRISL's relationship with Commerz Hamburg had grown to the point that IRISL was, by revenue, one of Commerz Hamburg's ten largest clients.

50. In January 2005, Commerz New York rejected a series of payments on behalf of Lancelin Shipping Company Ltd., an IRISL special purpose entity ("SPE"),⁴ registered in

⁴ An SPE is a type of corporate entity commonly used by shipping companies throughout the world to incorporate individual ships as a means of, among other things, limiting the liability of the parent company – that is, if a ship incurs a liability (e.g., from a crash or environmental disaster), those seeking damages are limited to the

Cyprus (these messages contained references to IRISL Europe GmbH, a wholly-owned IRISL subsidiary registered in Hamburg), and IRISL Europe GmbH due to the link to IRISL.

Commerz Hamburg Developed a "Safe Payments Solution" to Ensure that IRISL's Payments Were Not Delayed or Rejected in the United States

51. On January 24, 2005, after Commerz New York had rejected the payments, one of the relationship managers in the Hamburg branch of the Bank met with employees from IRISL. A memorandum summarizing the meeting noted that IRISL "is looking for a possibility to conduct its payments without interruption." The Commerz relationship manager noted, "[d]ue to the tense political relations between Iran and the U.S., sanctions that have existed for some years against Iran and Iranian companies have been tightened." Specifically, with respect to IRISL, the memorandum observed, "**The number of rejected payments recently increased sharply since the word "IRISL" results in inquiries at foreign banks.** Based on inquiries from Commerzbank, New York we assume that it appears as a term on the embargo list." (Emphasis in original.)

52. In order to avoid having IRISL's payments stopped by Commerz New York, the Commerz relationship manager proposed a "safe payments solution." Specifically, any payment to or from IRISL that would otherwise trigger U.S. sanctions instead would be routed through accounts in the name of either Lancelin Shipping Company Ltd. or Company 1, IRISL SPEs. Crucially for Commerz, U.S. sanctions filters would not catch Company 1 and Lancelin because they appeared to be Cypriot companies with no apparent connection to IRISL or Iran. Because, under the "safe payment solution," Company 1 and Lancelin received payments wholly unrelated to them, Commerz zeroed out the balance of Company 1's and Lancelin's accounts on a daily

assets of the SPE. IRISL created and used a number of subsidiary SPEs, which it domiciled and registered in Malta and Cyprus.

basis and transferred the funds to accounts held in the name of IRISL Europe GmbH pursuant to a cash pooling agreement.

53. The Commerz relationship manager detailed the mechanics of the “safe payments solution” in a written presentation that he delivered to IRISL on January 25, 2005, noting that “[t]he current rejections show that IRISL is in the OFAC list” (emphasis in original). The presentation explained that “payments which are sent through a . . . subsidiary are unlikely to be rejected to our present knowledge.” The Commerz relationship manager explained that he sent the presentation “to visualize our thoughts regarding a ‘safe payments’ solution which would reduce the returned payments and the danger of funds frozen by US bankers due to existing restrictions.”

54. An email chain from May 2005 demonstrates how the “safe payments solution” was used to process USD transactions and also describes how both IRISL and Commerz employees violated U.S. sanctions. On or about May 18, 2005, IRISL and Commerz employees learned that a payment from IRISL Europe GmbH to a bank in Moscow, Russia, had been rejected because the branch was a wholly-owned subsidiary of a U.S. bank. On or about May 23, 2005, a Commerz relationship manager for IRISL advised IRISL employees to resubmit the payment, to “make this a safe payment b/o [by order] of Lancelin or [Company 1].”

55. Commerz Hamburg and IRISL switched the use of SPEs when OFAC filters were updated to detect the use of a particular SPE. On January 10, 2006, Commerz New York rejected a USD payment to Company 1 and notified Commerz Frankfurt Compliance. On January 24, 2006, an IRISL employee emailed other IRISL employees an instruction that they should stop using the Company 1 account for “safe payments” and instead should use the Lancelin account, copying a relationship manager from Commerz Hamburg on the email.

Similarly, on April 18, 2006, Commerz New York rejected a payment on behalf of Lancelin, citing "US sanctions against Iran." Three months later, on July 19, 2006, an IRISL relationship manager at Commerz communicated a change in the structure of the "safe payment solution." Company 1 and Lancelin would no longer receive payments on behalf of IRISL and IRISL Europe GmbH. Instead, two other IRISL SPEs were to be used for processing payments on behalf of IRISL and IRISL Europe GmbH.

56. Commerz charged IRISL more money for this special "safe payment" service. On February 1, 2005, an IRISL relationship manager at Commerz emailed IRISL employees regarding proposed fees for transactions. The relationship manager proposed charging, in general, five Euros for each foreign payment. But for foreign payments sent as part of the "safe payment solution," the employee proposed charging 20 Euros, noting that, "[b]y providing no details which are current[ly] subject to the OFAC embargo database, the risk of payments being frozen or rejected by US banks or their subsidiaries will be significantly reduced."

57. Supervisors in Commerz's Hamburg office knew of and condoned the "safe payments solution." For example, in March 2005, Commerz New York began raising questions about Company 1's connection to IRISL. On March 10, 2005, a Hamburg relationship manager for IRISL prepared a draft response to Commerz New York in which the relationship manager acknowledged that IRISL was a shareholder of Company 1. The relationship manager's supervisors, however, reviewed the response and instructed him to remove the information that IRISL was a Company 1 shareholder. Ultimately, after additional questions from Commerz Frankfurt about the connection between Company 1 and IRISL, Commerz Hamburg revealed Company 1's connection to IRISL to the Frankfurt Compliance officer, who, in turn, shared the response with Commerz New York. Commerz New York added Company 1 to its OFAC filter.

Commerz New York Escalated Concerns Regarding Commerz Hamburg's Conduct

58. In the first half of 2006, Commerz Frankfurt replaced certain Compliance personnel, including the Global Head of Compliance.

59. On or about June 27, 2006, in response to a request from the new Global Head of Compliance, the Head of Commerz New York's Compliance Department emailed members of her team, asking if there were any concerns they wanted her to share with the new Global Head of Compliance. One of Commerz New York's Compliance employees responded with several items, one of which was "[p]ersistent disregarding of OFAC rules by foreign branches. Hamburg is notorious for it." In an interview with federal and state investigators, the Head of Commerz New York Compliance explained that in her meeting with the Global Head of Compliance, she generally shared her department's concern with sanctions compliance at foreign branches.

OFAC Raised Concerns About Commerz's Relationship with IRISL and Designated IRISL As an SDN

60. On or about July 15, 2008, the Head of Commerz's Global Compliance, the Head of Global Sanctions, the Head of Commerz New York's Compliance, and outside counsel for the Bank met with a number of officials from OFAC in Washington, D.C. Commerz's Head of New York Compliance took notes of the meeting. According to the notes, OFAC "appeared taken aback to hear that IRISL remained a [Commerz] Customer."

61. On or about September 10, 2008, OFAC placed IRISL, IRISL Europe GmbH, and several IRISL SPEs on its SDN list based on evidence that the IRISL family of companies was engaged in weapons of mass destruction proliferation activity. In the press release announcing the designation, OFAC noted "[n]ot only does IRISL facilitate the transport of cargo for U.N.

designated proliferators, it also falsifies documents and uses deceptive schemes to shroud its involvement in illicit commerce. . . . IRISL's actions are part of a broader pattern of deception and fabrication that Iran uses to advance its nuclear and missile programs." OFAC advised that "as international attention over Iran's [Weapons of Mass Destruction] programs has increased, IRISL has pursued new strategies which could afford it the potential to evade future detection of military shipments." OFAC warned that "[t]hese designations also highlight the dangers of doing business with IRISL and its subsidiaries. Countries and firms, including customers, business partners, and maritime insurers doing business with IRISL, may be unwittingly helping the shipping line facilitate Iran's proliferation activities."

62. On or about September 11, 2008, a senior official at OFAC personally forwarded the press release announcing IRISL's SDN designation to the Head of Compliance at Commerz New York. And, on or about September 11, 2008, a Commerz relationship manager for IRISL forwarded OFAC's press release to several Commerz Hamburg employees with responsibilities related to IRISL. In the email, the relationship manager noted that the penalties were "directed toward IRISL and their subsidiaries" and that the U.S. government alleged "that IRISL as Iranian government carrier systematically circumvents the Iranian arms embargo."

After IRISL, IRISL Europe GmbH, and Several IRISL SPEs and Related Entities Were Designated as SDNs by OFAC, Commerz Continued to Process USD Payments on Behalf of Known IRISL Entities

63. Notably, throughout the relevant period, Commerz employees who had responsibilities related to IRISL viewed IRISL, IRISL Europe GmbH, and all of the IRISL subsidiaries and related entities, including IRISL SPEs, as one single customer. In interviews with federal and state investigators, employees consistently confirmed that the Bank's internal metrics treated IRISL and all of its subsidiaries and related entities collectively as one customer

group. As such, several employees who had IRISL-related responsibilities at Commerz told federal and state investigators in interviews that they assumed that once IRISL and IRISL Europe GmbH were designated, all IRISL entities were designated.

64. Nonetheless, Commerz continued handling USD business on behalf of IRISL subsidiaries and related entities after IRISL had been designated by OFAC as an SDN.

65. Between September 10, 2008, and December 31, 2008, Commerz transmitted payment messages, totaling approximately \$39,567,720 in value, many of which were on behalf of IRISL subsidiaries and related entities through Commerz New York, or other U.S. financial institutions that had a U.S. connection, or that flowed through the United States after the revocation of the U-turn exemption. All of these payments (which were in addition to the other Iranian payments described above) were processed in violation of IEEPA and ITRs, and caused false entries to be made in the business records of financial institutions located in New York, New York.

Sudan

66. Commerz also conducted a significant amount of business with Sudan in violation of U.S. sanctions. Notably, there has never been a U-turn exemption for Sudanese payments. Thus, at relevant times all USD payments on behalf of Sudanese clients that terminated in, flowed through, or were otherwise connected to the United States were prohibited by IEEPA and SSRs, unless specifically exempted or licensed by OFAC.

67. Generally, the illegal Sudanese payments were processed using the non-transparent cover payment method, which ensured that the U.S. clearing bank (Commerz New York) received a payment message that did not include originator or beneficiary information.

68. As it had done for certain of its Iranian clients, Commerz instructed Sudanese banks on how to evade U.S. sanctions. For example, on August 2, 2001, the Commerz relationship manager for Sudan—a member of Middle Management—sent a letter to a Sudanese bank explaining that when the customer wanted to receive a USD payment that had to clear through the United States the payment should be structured as a cover payment, and that “[i]t is very important that the [cover payment] does not mention your bank as beneficiary nor make any other reference to Sudan, to avoid the funds are blocked in New York.” (Emphasis in original.) In an interview with federal and state investigators, the relationship manager explained that it was his understanding that the transaction would be rejected or blocked in the United States if this information were revealed to a U.S. bank and that he provided this advice in an effort to ensure the customer payments were not rejected or blocked. The Sudanese relationship manager also orally instructed employees at Sudanese banks to avoid mentioning Sudan in payments that transited through the United States.

69. Commerz also structured payment messages to prevent Commerz New York from identifying payments as involving Sudan and therefore enforcing U.S. sanctions to stop payments. For example, on August 19, 2005, a member of Commerz’s Back Office contacted a Commerz Frankfurt Compliance officer about a USD transaction involving a letter of credit for a Sudanese SDN bank. The Back Office employee outlined how he intended to structure the payment and sought confirmation that the proposed structure would not cause any problems with the transaction being processed in the United States. The Commerz Frankfurt Compliance officer responded, “[a]s long as the Sudan background or notify address is not visible in payments to the U.S., the statement [that the Sudanese background would not be visible to the United States] is accurate.”

70. Commerz continued to clear Sudanese USD transactions through the United States despite knowing that these transactions were illegal under U.S. law. In an August 2005 memorandum from the Compliance and Legal departments, the Board members were informed of external counsel's July 2005 legal opinion on cover payments, which made clear that the Bank could not use cover payments to effect unlawful Sudanese payments. Knowledge of this opinion eventually filtered down to lower level Commerz employees, and on September 19, 2005, the Commerz relationship manager for Sudan sent a memorandum to another Financial Institutions employee acknowledging that the practice of using cover payments to circumvent U.S. sanctions was illegal: "In the past the blocking of [Sudanese] funds used to be occasionally avoided by the transmission of an MT 202. This does not reveal the sender so that the U.S. American authorities do not recognize the background and hence the funds are not blocked. This procedure is, according to the U.S. American opinion, illegal[.]" Despite the fact that Senior Management was unequivocally informed in August 2005 that these Sudanese cover payments were unlawful, these transactions persisted until April 10, 2006, when the Bank ultimately announced that all USD accounts involving Sudanese clients should be closed.

71. Between January 1, 2002, and December 31, 2007, Commerz transmitted payment messages, totaling approximately \$183,428,000 in value, through Commerz New York in violation of IEEPA and SSRs, and caused false entries to be made in the business records of financial institutions located in New York, New York. Of these payment messages, approximately \$35,071,000 of the payments were on behalf of, or involved, SDNs.

Other Sanctions Violations

72. The Bank also conducted business involving client SDNs located in countries other than Iran and Sudan in violation of IEEPA and New York State laws.

73. Between January 1, 2002, and December 31, 2007, Commerz transmitted payments on behalf of, or involving, Cuban SDNs, totaling approximately \$3,557,000, through Commerz New York or other U.S. financial institutions in violation of IEEPA and New York State laws.

74. Between January 1, 2002, and December 31, 2007, Commerz transmitted payments on behalf of, or involving, Burmese SDNs, totaling approximately \$2,711,000, through Commerz New York or other U.S. financial institutions in violation of IEEPA and New York State laws.

75. Between January 1, 2002, and December 31, 2007, Commerz transmitted payments totaling approximately \$2,019,000, through Commerz New York or other U.S. financial institutions in violation of IEEPA and New York State laws on behalf of SDNs not affiliated with Iran, Sudan, Cuba, or Burma.

Commerz's Internal Investigation

76. Throughout the course of this investigation, Commerz has cooperated with U.S. authorities. Commerz undertook a voluntary and comprehensive internal review of its historical payment processing and sanctions compliance practices, which has included the following:

- a. An extensive review of records, including hard copy and electronic documents;
- b. Numerous interviews of current and former employees;
- c. A transaction review conducted by an outside consultant, which included, but was not limited to review of millions of payment messages and trade transactions across various accounts related to sanctioned countries, including an analysis of underlying SWIFT transmission data associated with USD activity for accounts of banks in sanctioned countries;

- d. Regular and detailed updates to DANY and DOJ on the results of its investigation and forensic SWIFT data analyses, and responding to additional specific requests for information and investigation of DANY and DOJ;
- e. A detailed written report of the Bank's investigation;
- f. Agreements to toll any applicable statutes of limitation by Commerz and by its subsidiary, Commerzbank International S.A. Luxembourg;
- g. Partial waiver of the attorney-client privilege; and
- h. Making numerous current and former Commerz employees available for interviews by U.S. authorities in Europe, New York, and Washington D.C.

Commerz's Remediation

77. Commerz has also taken voluntary steps to enhance and optimize its sanctions compliance programs, including by:

- a. Installing more sophisticated filtering software and testing, improving and fine-tuning its transaction monitoring software;
- b. Hiring numerous additional senior and junior compliance employees with extensive sanctions-related expertise;
- c. Enhancing written compliance policies that address U.S. sanctions against Iran, Burma, North Korea, Sudan, and Cuba;
- d. Enhancing its transactions monitoring and client on-boarding due diligence, including from an OFAC perspective;
- e. Enhancing its trade finance due diligence protocols;
- f. Implementing extensive compliance training; and

- g. Retaining several outside consultants to help the Bank assess and further improve existing compliance programs and strategies, including with respect to correspondent banking.

78. Commerz has also agreed, as part of its cooperation with DANY and DOJ, to complete the ongoing work necessary to further enhance and optimize its sanctions compliance programs. Commerz has also agreed to cooperate in DANY and DOJ's ongoing investigations into these banking practices and has agreed to continue to comply with the Wolfsberg Anti-Money Laundering Principles of Correspondent Banking.

ATTACHMENT B

[BSA/AML Statement of Facts]

INTRODUCTION

1. The following Statement of Facts is incorporated by reference as part of the deferred prosecution agreement (the "Agreement") between the United States Attorney's Office for the Southern District of New York; the United States Attorney's Office for the District of Columbia; and the United States Department of Justice, Criminal Division, Asset Forfeiture and Money Laundering Section, on the one hand, and Commerzbank AG ("Commerz" or the "Bank") and its New York branch ("Commerz New York"), on the other.

2. The parties agree and stipulate that the information contained in this Statement of Facts is true and accurate. Commerz and Commerz New York agree that, if this matter were to proceed to trial, the United States Attorney's Office for the Southern District of New York would prove beyond a reasonable doubt, by admissible evidence, the facts described herein and set forth in the criminal Information attached to this Agreement.

Bank Background

3. Commerz conducts business in Europe, North America, and Asia; in addition, it has representative offices in South America, Africa, and Australia. Commerz is headquartered in Frankfurt, Germany, and has over 1,200 branches in Germany alone. Commerz is represented outside Germany by 23 foreign branches—including, as discussed below, in Singapore and in New York, New York—35 representative offices and a number of subsidiaries, spread across more than 50 countries. Commerz is listed on exchanges in Germany, London, and Switzerland, and its shares can be purchased in the United States through American Depositary Receipts.

4. Since 1971 Commerz has had a license issued by the state of New York to operate as a foreign bank branch in New York, New York. The branch provides U.S. dollar clearing for international wire payments and provides banking services to German companies, subsidiaries of German companies located in the United States, and U.S. companies.

5. For many years, Commerz's investment banking operations were offered through Commerzbank Capital Markets Corp., a separate legal entity from Commerz. That business unit was liquidated. However, after Commerz acquired Dresdner Bank AG ("Dresdner") in 2008, it resumed offering investment banking services through the former Dresdner Kleinwort Securities LLC, which was renamed Commerz Markets LLC.

Commerz's Correspondent Banking Business

6. At all times relevant to this Statement of Facts, Commerz New York operated a correspondent banking business for purposes of offering the Bank's foreign clients U.S. dollar clearing services. In addition, Commerz New York offered correspondent banking services for other foreign financial institutions.

7. Correspondent accounts are established at banks to receive deposits from, and make payments on behalf of, or handle other financial transactions for other financial institutions, including foreign financial institutions. Correspondent banking involves the facilitation of wire transfers between foreign financial institutions and their customers, and other financial institutions with which the foreign financial institution does not have a direct relationship.

8. Correspondent accounts are generally considered to be higher risk than other banking accounts, because the bank does not have a direct relationship with, and therefore has no diligence information on, the correspondent financial institution's customers who initiated the wire transfers. To mitigate this risk, as set forth below, U.S. law requires financial institutions to conduct due diligence on all non-U.S. entities (*i.e.*, the foreign financial institutions) for which it maintains correspondent accounts. There is no exception for foreign financial institutions within the same parent company; that is, for branches and affiliates of the same bank.

9. At all times relevant to this Statement of Facts, Commerz New York maintained correspondent accounts for a number of non-U.S. financial institutions, including certain affiliates and non-U.S. branches of Commerz. Commerz is a member of the Society for Worldwide Interbank Financial Telecommunications (“SWIFT”) and historically has used the SWIFT message types and/or system to transmit international payment messages to and from other financial institutions around the world, including Commerz New York.

10. Transactions in U.S. dollars between two individuals or entities who reside inside or outside the United States and who maintain accounts at different non-U.S. banks typically must transit through the United States through correspondent accounts and through the use of SWIFT messages. This process is typically referred to as “clearing” through U.S. correspondent banks.

**COMMERZ NEW YORK'S FAILURE TO
REPORT SUSPICIOUS ACTIVITY, MAINTAIN AN EFFECTIVE ANTI-MONEY
LAUNDERING PROGRAM AND CONDUCT DILIGENCE ON CORRESPONDENT
ACCOUNTS**

Applicable Law

11. The Currency and Foreign Transactions Reporting Act of 1970 (commonly known as the Bank Secrecy Act, or “BSA”), Title 31, United States Code, Section 5311, *et seq.*, requires financial institutions—including a “commercial bank” or a “branch of a foreign bank in the United States,” 31 U.S.C. § 5312(a)(2)—to take certain steps to protect against the financial institution being used by criminals to commit crimes and launder money.

12. In the United States, the Board of Governors of the Federal Reserve System is the federal banking agency supervisor of Commerz. By virtue of its operations in the United States, Commerz is subject to the requirements of the BSA, and the associated regulations promulgated by the Department of the Treasury and the Federal Reserve.

13. The BSA requires financial institutions to establish and maintain effective anti-money laundering (“AML”) compliance programs that, at a minimum and among other things, provide for: (a) internal policies, procedures, and controls designed to guard against money laundering; (b) an individual or individuals to coordinate and monitor day-to-day compliance with BSA and AML requirements; (c) an ongoing employee training program; and (d) an independent audit function to test compliance programs. 31 U.S.C. § 5318(h).

14. Pursuant to Title 31, United States Code, Section 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 subject such accounts to “enhanced scrutiny” to detect and report suspicious activity. The due diligence program, among other things, was required to include “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 suspect money laundering activity conducted through or involving any correspondent account.” 31 C.F.R. § 1010.610(a). Financial institutions are also required to “[m]onitor[] transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity,” including obtaining information about the identity of the ultimate sender or recipient of the funds. 31 C.F.R. § 1010.610(b)(1)(ii) & (iii)(A).

15. For foreign correspondent accounts, the implementing regulations require that the due diligence requirements set forth in Section 5318(i)(1) include an assessment of the money laundering risk presented by the account based on all 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 AML and supervisory regime of the jurisdiction issuing the license for the account holder; and (v) information reasonably available about the account holder's AML record. There is no exception to the due diligence requirement for correspondent accounts held by foreign financial institutions with the same parent company, such as foreign branches or affiliates of the U.S. financial institution.

16. The BSA and regulations thereunder also require financial institutions to report "suspicious transaction[s] relevant to a possible violation of law or regulation." 31 U.S.C. § 5318(g)(1). BSA regulations provide that a transaction is reportable if it is "conducted or attempted by, at, or through the bank" and where "the bank knows, suspects, or has reason to suspect that . . . [t]he transaction involves funds derived from illegal activities" or that the "transaction has no business or apparent lawful purpose." 31 C.F.R. § 1020.320(a)(2). A separate BSA regulation provides that a bank must file a Suspicious Activity Report ("SAR") where the bank "detects any known or suspected Federal criminal violation, or pattern of criminal violations . . . aggregating \$5,000 or more in funds or other assets . . . where the bank believes that . . . the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects." 12 C.F.R. § 208.62(c)(2). If the transactions total more than \$25,000, then a bank must file a report even if it cannot identify a suspect. 12 C.F.R. § 208.62(c)(3). Financial institutions satisfy their obligation to report such a transaction by filing a SAR with the Financial Crimes Enforcement Network ("FinCEN"), a part of the United States Department of Treasury. 31 C.F.R. § 1020.320(a)(1).

The U.S. Attorney's Office for the Southern District of New York's Charge

17. The United States Attorney's Office for the Southern District of New York has alleged, and Commerz and Commerz New York both accept, that Commerz New York's conduct, as described herein, violated Title 31, United States Code, Sections 5318(g), 5318(h), 5318(i), and 5322(b) & (c), because Commerz New York, acting through certain employees located in New York, willfully (i) failed to maintain an adequate anti-money laundering program, (ii) failed to establish due diligence for foreign correspondent accounts; and (iii) failed to report suspicious transactions relevant to a possible violation of law or regulations, as required by the Secretary of the Treasury.

Conduct in Violation of the BSA

18. From at least in or about 2008, and continuing until 2013, Commerz New York, acting through certain employees located in 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 U.S. law, including its obligations to detect and report suspicious transaction activity. As a result of the willful failure of Commerz New York to comply with U.S. law, a multi-billion dollar securities fraud was operated through the Bank and other reportable transactions under U.S. law were never detected.

19. There were at least three significant failures in Commerz New York's AML program that allowed transactions in the proceeds of fraud and other suspicious transactions to be processed through Commerz New York:

- a. Failure to adequately conduct investigations of transactions that were deemed potentially suspicious or that "alerted" in the Bank's automated AML software, instead closing AML investigations based on no or faulty information received in response to requests for information.

- b. Failure to report suspicious activity, including more than \$1.6 billion in wire transfers through Commerz New York that ultimately furthered the massive accounting fraud at the Olympus Corporation.
- c. Failure to adequately monitor billions of dollars in correspondent banking transactions, including by failing to conduct due diligence or enhanced due diligence on Commerz affiliates and branches, including the head office in Frankfurt and Commerz's Singapore branch ("Commerz Singapore").

20. In addition, business units at CommerzBank AG in Frankfurt, did not permit the U.S. AML compliance program to act independently from the bank's business or from compliance personnel in Frankfurt (who were not responsible for U.S. law compliance), by, for example, insisting on the restoration of correspondent accounts that had been blocked for AML reasons by U.S. AML compliance personnel.

21. As described in more detail below, on October 16, 2013, the Board of Governors of the Federal Reserve System issued a Cease and Desist Order to Commerz and Commerz New York based on the failures of its BSA/AML compliance program in the correspondent banking business.

**Commerz New York Failed to Conduct Due Diligence on Commerz,
and its Branches and Affiliates**

22. Group Compliance at Commerz had overall responsibility for ensuring the Bank's legal and regulatory compliance throughout the world. At all relevant times, Group Compliance was supervised by the Bank's Global Head of Compliance (the "Global Head of Compliance"), who was located in Frankfurt, Germany. Commerz New York's compliance department had primary responsibility for the Bank's compliance with U.S. law, including the BSA, and reported to the Global Head of Compliance. As the Bank recognized in an internal audit report of its

AML program, the compliance group in New York “has oversight responsibility to ensure that all U.S. related customers and transactions are monitored considering all relevant U.S. AML regulations.”

23. At all relevant times, as required by the BSA, Commerz designated an executive located in New York, New York (the “Commerz BSA Officer” or the “BSA Officer”) as the head of Commerz’s AML program and the individual ultimately responsible for ensuring Commerz’s ongoing compliance with its BSA obligations, including the filing of SARs when required. In or about August 2008, in connection with the merger and integration of Dresdner, the BSA Officer was replaced as head of compliance in New York, a position she briefly held, but the BSA Officer retained her responsibilities under the BSA until at least early 2014, even as she reported to the new head of compliance.

24. During the relevant time period, Commerz New York correctly considered other Commerz branch offices and affiliates to be foreign financial institutions for purposes of the BSA, such that it maintained correspondent banking accounts for its own foreign branches and affiliates. For example, Commerz’s Singapore branch maintained a correspondent account in New York, which allowed customers of Commerz Singapore to engage in U.S. dollar transactions through Commerz New York.

25. Commerz New York, however, did not conduct due diligence or assign any risk-rating to the other Commerz branches and affiliates until approximately 2007, when it came under criticism from the Federal Reserve Bank of New York (“FRBNY”). At that point, Commerz New York began to conduct due diligence of its affiliates, but not its branches. It was not until 2013, at or about the time when Commerz New York was criticized by the FRBNY for failing to conduct due diligence or enhanced due diligence of its branches (specifically, on the

head office in Frankfurt), that it began to do so. (As discussed below, the FRBNY found in the 2013 review that the due diligence of Commerz affiliates was inadequate.) Nor did Commerz New York (as was consistent with industry practice) have direct access to information about the foreign branches' clients, such that it could identify the ultimate sender or recipient of funds that flowed through its correspondent accounts. In many cases, transactions through the Commerz New York correspondent accounts were accompanied by SWIFT messages which did not allow the identity of the payer or recipient to be included in the message. But even where Commerz New York was aware of the ultimate client of the foreign Commerz branch or affiliate, it did not have direct access to information about that client.

26. Rather, until approximately 2013, virtually all AML-related customer information—including so-called “know your customer” (or KYC) material and enhanced due diligence material—was maintained at Commerz Frankfurt, and Commerz New York lacked physical access to such material. (The only exception was for the relatively small number of non-correspondent banking customers that were clients of Commerz New York itself.)

27. Commerz relied on a computerized system to comply with its AML obligations. Specifically, with respect to correspondent accounts, Commerz employed software tools commonly used by large financial institutions to monitor account activity. Among other things, these software tools sought to determine how an account's activity compared to “peer” accounts and whether the account in question was behaving uncharacteristically for the peer group in terms of the value of the account and the volume of transactions.

28. Correspondent accounts at Commerz New York, however, were not effectively monitored using many of these tools until late 2009 because, among other things, the SWIFT format prevented the inclusion of all necessary information about the ultimate sender and

beneficiary of the transfer, and because there was no risk-rating for the correspondent account. Even after November 2009, when SWIFT introduced a new messaging format that required the ultimate sender and recipient of funds to be identified, Commerz New York was unable to effectively monitor the transactions in its correspondent business because Commerz lacked risk-ratings and other due diligence information about its own foreign branches and affiliates. Prior to that, Commerz New York conducted keyword searches of correspondent bank transfers that could identify a suspicious sender or recipient—if the payment information included a sender or recipient—but which could not otherwise effectively detect suspicious activity.

29. Even though Commerz New York was not conducting due diligence or enhanced due diligence of its own branches and affiliates, senior Commerz officials, including the Global Head of Compliance, were well aware that certain subsidiaries of Commerz in Singapore serviced customers who were engaged in potentially high-risk activities. For example, the Bank's Global Head of Compliance understood that the private banking business in Singapore, known as Commerzbank (Southeast Asia) Ltd. ("COSEA"), and a trusts business in Singapore, Commerzbank International Trust (Singapore) Ltd. ("CITS"), serviced high-risk customers. With respect to COSEA, the Global Head of Compliance understood that a German bank that predominately services German clients would not be an obvious choice for high-net worth individuals in a location like Singapore. Such clients were likely to go to the largest international banks. The next tier of clients were likely to go to reputable local banks. But as the Global Head of Compliance explained to federal investigators, the kind of clients who would go to COSEA (other than certain German expatriates) were higher risk. That was particularly so, the Global Head of Compliance explained, because Singapore is a known tax haven due to its strict bank secrecy laws. Indeed, the Global Head of Compliance was sufficiently concerned

about the risks associated with COSEA that he sent compliance employees to assess the risk of the business and ultimately supported its closure, a process that was completed by April 2011 (approximately 6 months before the Olympus fraud was revealed). And although his concerns related principally to COSEA, it was understood that any U.S. dollar denominated transfers on behalf of COSEA clients would necessarily be cleared through the Singapore branch's correspondent account at Commerz New York, raising the branch's risk profile, as well. Nonetheless, Commerz New York failed to conduct due diligence or enhanced due diligence of Commerz's Singapore branch, or to assign it a risk-rating, until approximately 2013.

Commerz New York Failed to Adequately Investigate AML Alerts

30. In the event that the computerized AML systems generated an "alert," Commerz policy provided that an AML compliance officer would investigate the alert and take appropriate action—which could include searching public sources and internal KYC materials, contacting business people at the Bank, or contacting compliance personnel in Frankfurt or at a foreign branch—if any action was required.

31. Because the KYC and enhanced due diligence materials for foreign branches and their clients were housed at Commerz Frankfurt, AML compliance officers in New York had no physical access to those materials. Rather, whenever a transaction "alerted" in the automated transaction monitoring software, or an AML investigation had to be conducted for any other reason, Commerz New York was required to submit a request for information to its counterparts in Frankfurt. Where compliance personnel in New York had preexisting relationships with compliance personnel in other Commerz branches, they could also send a request for information directly to the foreign branch.

32. As discussed further below, Commerz Frankfurt was repeatedly criticized—by its primary federal regulator and even by its own BSA Officer—for failing to timely and completely

provide information responsive to such requests. Even when Commerz New York compliance officials did receive a response from Frankfurt or from other Commerz branches, that information was frequently incomplete or insufficient. From time to time following the 2009 Dresdner acquisition, Commerz New York had more than one hundred outstanding requests for information, and sometimes waited for as long as eight months for a response. When responses were received, they were often inadequate.

33. As a result of these deficiencies, Commerz New York cleared numerous AML “alerts” based on its own perfunctory internet searches but without ever receiving responses to its requests for information. Commerz New York therefore processed hundreds of millions of dollars in transactions that other parts of the Bank may have deemed to be suspicious without ever alerting U.S. regulators or filing a SAR.

Commerz New York Failed to Report Suspicious Activity, Such as the Accounting Fraud Perpetrated by the Olympus Corporation

34. At all relevant times, 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.

35. From 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—including its Chairman, an executive vice president, and its general auditor—pleaded guilty in Japan to inflating the company’s net worth by approximately \$1.7 billion.

36. As described below, Olympus, through false representations made by Olympus executives, used Commerz to perpetrate its fraud. Among other things, the fraud was perpetrated by Olympus through special purpose vehicles, some of which were created by Commerz—

including several executives based in Singapore—at Olympus’s direction, using funding from Commerz. One of those Singapore-based executives, Chan Ming Fon—who was involved both in creating the Olympus structure in 1999 while at COSEA, and who later on his own managed an Olympus-related entity in 2005-2010 on behalf of which Chan submitted false confirmations to Olympus’s auditors—subsequently pleaded guilty in the United States District Court for the Southern District of New York to conspiracy to commit wire fraud.

37. Although Olympus executives deceived Commerz about the true purpose of these transactions—including the Commerz-created special purpose vehicles and hundreds of millions of dollars in Commerz loans—between approximately 1999 and 2008, numerous Commerz executives nonetheless developed suspicions about the Olympus transactions. And despite those suspicions, which in 2008 were shared with, among others, the Bank’s Global Head of Compliance in Frankfurt, Commerz New York processed hundreds of millions of dollars in wires which, while unknown to Commerz, were in furtherance of the scheme.

38. Prior to November 2009, when the new SWIFT messaging format that included mandatory sender/beneficiary information was introduced across the industry, Commerz New York often had no understanding of who the parties to the Olympus-related transactions were. When, in or about 2010, Commerz New York’s automated transaction monitoring software “alerted” on certain Olympus-related wires and New York-based compliance officials specifically inquired about the purpose of the transfers, none of the Bank’s suspicions—or the underlying facts—were shared with Commerz New York. Instead, Commerz New York’s inquiry was answered by a two-sentence e-mail which eventually led to the clearing of the Olympus alerts in New York. Between 1999 and 2010, the New York branch processed more

than \$1.6 billion in transfers orchestrated by Olympus in furtherance of the Olympus accounting fraud.

The Mechanics of the Olympus Fraud

39. In the 1980s and 1990s, Olympus made a number of financial investments unrelated to its core device manufacturing business, which were designed to boost its earnings. Rather than increase earnings, however, the investments lost hundreds of millions of dollars. Because Japanese accounting standards permitted Olympus to account for the investments on a cost basis, however, Olympus's financial statements did not reflect the sizeable unrealized losses.

40. In the late 1990s, however, Japanese accounting standards changed and required the investments to be accounted for at fair value. Rather than realize the losses, Olympus executives devised a scheme to conceal the losses from Olympus's investors and auditors. The scheme, which at various times involved a variety of trusts and special purpose vehicles, worked essentially as follows in its earlier incarnation: Olympus created off-balance-sheet special purpose vehicles (or SPVs), which received a sizeable loan from a recognized financial institution. The loan was secured by Olympus's cash on deposit at the financial institution. The special purpose vehicles then purchased Olympus's losing investments at book value (rather than at fair market value), allowing Olympus to avoid realizing the loss. At the same time, Olympus serviced the loan. As a result, Olympus was able to move the investments off its balance sheet and replace them with cash equivalent to their book value, while also keeping the corresponding liability (*i.e.*, the bank loan) off its balance sheet, as well—which had the end result of falsely overstating Olympus's assets by omitting the investment losses. Olympus officials intended to (and did) spread the losses over a period of years, and hid them in other events—such as restructurings or depreciation of other assets—where they would not be noticed.

41. Critical to this version of the scheme, Olympus did not disclose that its cash on deposit was encumbered as collateral for the bank loans to the SPVs, creating the false impression that Olympus's investment assets were valuable and that it had significant cash on hand. In reality, the investment assets had suffered hundreds of millions of dollars in losses, and Olympus's large cash deposits were pledged to secure bank loans. As described below, later versions of the scheme did not involve the use of a bank loan, but the point was always the same: to conceal the significant losses sustained by Olympus in its investment portfolio.

42. All told, Olympus falsely inflated its assets by approximately \$1.7 billion, over a period of approximately a decade.

Suspicious at Commerz in 1999-2000

43. When the loan schemes were first conceived, Olympus turned to CITS (and other financial institutions in Europe and Japan) to help create the structure and supply the loan, aided by the COSEA relationship manager for Olympus, Chan Ming Fon. As documented in an August 23, 1999 memorandum from two senior officials at CITS, to unnamed "Sirs" at "Co.A," the purpose of the transaction was to "inject funds" into a "Cayman Islands company" referred to as "Co.B," and that "Co.A and Co.B would like the transfer of funds to be effected as an 'off-balance sheet' transaction," "with a reliable financial institution acting as an intermediary."

44. In fact, as the CITS officials knew, Co.A was Olympus, and Co.B was an Olympus-controlled entity called Twenty First Century Global Fixed Income Fund Ltd ("21 C"). Under the agreement, CITS created a charitable trust with a CITS affiliate acting as trustee, and a separate special purpose vehicle called Hillmore Investments Limited ("Hillmore"), which was to be wholly owned by the trust but administered by CITS, which would therefore provide a nominal shareholder, director, and corporate secretary, and which would execute all transactions on behalf of the SPV. Co.A (*i.e.*, Olympus) would then put cash on deposit at COSEA

(essentially Commerz's private bank in Singapore) equal to the amount of the desired loan, plus COSEA's fees and interest payments. COSEA, in turn, would extend the loan to Hillmore, secured by Olympus's deposits. Every time Hillmore drew down on the loan facility, 21 C (which had no relationship with any Commerz entity, including CITS and COSEA) was to issue notes, which Hillmore was to purchase with the loan proceeds. The agreement was signed by the Managing Director of CITS ("CITS Managing Director-1") and the Head of Business Development at CITS, and was counter-signed by two of the Olympus officials who ultimately pleaded guilty, Hideo Yamada and Hisashi Mori.

45. Pursuant to this agreement, COSEA in October 1999 and December 1999 loaned \$300 million to Hillmore, which was ultimately transferred through Commerz New York to 21 C, the Olympus-controlled, off-balance-sheet entity.

46. Virtually immediately, CITS personnel in Singapore recognized that the convoluted structure of this transaction was suspicious and raised questions about whether Olympus was properly disclosing to its auditors and/or investors the pledge of its cash collateral on deposit at COSEA. According to CITS Managing Director-1, CITS got "worried" when it began to get "signals" from Olympus about an unusual accounting treatment for the structure. After all, the sum total result of the structure was for Olympus to transfer its own cash to an entity it controlled. Olympus also paid loan interest and fees on those transfers to COSEA, as well as trust-related fees to CITS. The sole benefit to Olympus was to move the corresponding liability off of its balance sheet.

47. In September 2000, CITS Managing Director-1 wrote to senior Olympus officials and other participants in the structure, noting that CITS had been asked to sign a balance confirmation that did not disclose the fact that the cash on deposit was encumbered, "which will

presumably be given to [Olympus's] auditor." The CITS Managing Director wrote that "[o]ur bank is extremely uncomfortable with the formal and potential implications of signing the confirmation." He continued, "[b]y using the Secured bank loan/MTN [*i.e.*, note] structure, there does not appear to be any way around the client's [*i.e.*, Olympus's] obligation to make a note disclosure of the existence of the pledge," a reference to Olympus's pledge of collateral for the Hillmore loan.

48. But as CITS Managing Director-1 well knew (because, among other things, he was a signatory to the original agreement proposing the structure), the whole purpose of the arrangement was to keep the special purpose vehicle secret. Indeed, Olympus officials had (falsely) explained that the purpose of the structure was to allow Olympus to make secret, off-balance-sheet investments in competing endoscope manufacturers, in order to gain market share without alerting investors or the public about the investments. Thus, CITS executives were informed that Olympus wanted to keep the SPV, as well as its involvement in securing and servicing COSEA's loan to the SPV, secret. Had Olympus disclosed "the existence of the pledge," *i.e.*, that Olympus's cash deposits had been pledged as collateral for bank loans to the SPV, it would necessarily have revealed the existence of the SPV and defeated the purpose of the transaction. CITS Managing Director-1 continued in the September 2000 correspondence that "we are trying very hard to be accommodating to our client," but that "in order to protect against unintended outcomes to our Bank," Olympus needed to either disclose the pledge, change the structure, unwind the structure, or "absolv[e] us of the requirement to sign the confirmation."

49. In an e-mail written approximately a week later, CITS Managing Director-1 wrote to Mori at Olympus that CITS had received a legal opinion about the structure, which "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.” Nonetheless, CITS Managing Director-1 wrote that CITS was prepared to renew the agreement, so long as CITS was not required to be “a party to a misleading audit confirmation.”

50. As one possible solution to permit Olympus not to disclose the pledge, CITS Managing Director-1 suggested that Olympus could simply “repay[] the loan prior to year end”—when Olympus did its financial reporting— “with a new loan taken after year end,” to reinstate the structure. When interviewed by federal investigators, CITS Managing Director-1 said that Olympus was “not happy” when it learned that CITS would not sign a false audit confirmation, but that CITS was never required by Olympus to do so.

51. At approximately the same time, in the late summer of 2000, Chan Ming Fon—the Olympus relationship manager at COSEA who, along with other Bank employees, had originally helped conceive of the structure—left COSEA for another bank in Singapore (“Bank-2”). Shortly after the correspondence with CITS Managing Director-1, and after Chan left COSEA, Olympus also transferred its business to Bank-2, where it continued for the next several years before returning to CITS and COSEA.

52. CITS and COSEA earned approximately \$1.5 million in combined fees as a result of the Olympus-related business in 1999-2000.

The Fraud Returns to Commerz in 2005

53. After Olympus moved its business to Bank-2, Bank-2 replicated the structure that CITS and COSEA had participated in, this time with an Olympus-controlled entity called Easterside Investments Limited in the place of Hillmore. Bank-2 subsequently studied Olympus’s publicly-filed financial statements and, upon review, eventually withdrew from the structure at the end of 2004 by winding down its credit facility.

54. Also in or about 2004, Chan left Bank-2 and subsequently became the investment manager of an entity called SG Bond Plus Fund (“SG Bond”), which Chan established in the Cayman Islands in October 2004. SG Bond purportedly functioned as a private fund that invested primarily in low-risk bonds and fixed income securities. Beginning in early 2005, CITS became the administrator for SG Bond, as well as for another Chan Ming Fon controlled entity called Dynamic Dragon II SPC Sub Fund H. In early 2006, COSEA opened an account for SG Bond and another related entity called Global Target SPC Sub Fund H.

55. SG Bond quickly became part of the Olympus loss-hiding scheme. In early 2005, Olympus transferred approximately 60 billion yen to SG Bond, which SG Bond used to purchase an equivalent amount of relatively safe and marketable securities, such as Japanese government bonds, ostensibly for the benefit of Olympus. SG Bond then transferred those securities to Easterside, which sold the securities for cash and used the proceeds to, among other things, repay the loans from Bank-2.

56. The SG Bond investment portfolio, however, was on Olympus’s balance sheet, even though the assets purportedly held by SG Bond had in actuality been sold. From 2005 through at least 2009, Chan and others sent false documentation to Olympus’s auditors that failed to disclose that the 60 billion yen’s worth of securities had been transferred to Easterside and liquidated.

57. In or about 2010, Chan created another entity, to which Olympus again transferred hundreds of millions of dollars, which Chan used to purchase relatively safe securities such as the ones that he had purchased on SG Bond’s behalf in 2005. Upon acquiring the securities, Chan transferred them back to Easterside, which conveyed them to SG Bond, replacing the investment portfolio that SG Bond had purportedly held for Olympus since 2005.

Suspicious at Commerz in 2008

58. As noted above, CITS and COSEA became involved again in the Olympus structure beginning in or about 2005. At that time, CITS was run by a new managing director (“CITS Managing Director-2”), who had himself been present for and aware of the original Olympus/Hillmore structure in 1999-2000. Notwithstanding the Bank’s earlier concerns about the Olympus structure, CITS Managing Director-2 supported bringing the business back to Commerz, noting that it generated “substantial” fees for CITS.

59. In a memorandum dated August 29, 2008, however, CITS Managing Director-2 wrote to the COSEA Managing Director (who was also his boss), describing the SG Bond/Easterside/Olympus structure as “an off-balance sheet transaction for OC [*i.e.*, Olympus Corporation].” In an e-mail written at approximately the same time, CITS Managing Director-2 compared the structure to the “earlier appointment”—meaning the Hillmore structure from 1999-2000—and noted that “I was fully aware of the client’s intention which is an off-balance sheet structure.” CITS Managing Director-2’s memorandum raised a number of concerns about the Bank’s security and the possibility that Olympus would have to “write off full amount of USD500mio from their Balance Sheet,” along with resulting “[n]egative publicity” to CITS.

60. The memorandum concluded that “recently there were a number of scandal [*sic*] involving off balance sheet transactions where banks like Citibank are required to write off assets and those involved in structuring of such transaction are not mentioned.” A covering e-mail from CITS Managing Director-2 to the COSEA Managing Director reiterated that “my concern still remains, since this is a substantially large sum and reputational risk for Commerzbank AG group, if client has to write off this amount from their books. How will the main Board or your boss react to this if any negative news is splash on the front page news with involvement of

Commerzbank?” The COSEA Managing Director replied that CITS Managing Director-2’s e-mail and memorandum were “dishonorable.”

61. In or about early 2008, COSEA faced regulatory criticism for its AML compliance program and its maintenance of high-risk customer accounts. Among other things, COSEA was criticized for failing to correct a number of deficiencies that had been identified after a similar review some years earlier. As a result, in July 2008, Commerz’s Global Head of Compliance decided to dispatch a senior compliance officer from London (the “London Compliance Officer”) to Singapore to, among other things, address the concerns raised in the critical review and to assist COSEA and CITS “in [their] identification of clients that present an unacceptable regulatory risk to the Commerzbank Group.”

62. Upon arriving in Singapore, the London Compliance Officer was advised by the then-Head of Legal and Compliance for Asia (“Asia Compliance Head-1”) to look at, among other clients, the Olympus-related entities. Asia Compliance Head-1 noted in a September 10, 2008 e-mail that the structures were “complex” and “extraordinarily elaborate and redolent of layering,” and suggested the London Compliance Officer look at them closely. He continued that “[t]he present status is that the structures and transactions give rise to suspicion of ML [*i.e.*, money laundering] unless they can be adequately explained by the business. I am concerned about fraud, asset stripping, market manipulation and derivative Tax offences. . . . If the structure and transactions cannot [be] explained we must file Suspicious Transaction report [*sic*] as a matter of law and ZGC [*i.e.*, Group Compliance] policy.” Asia Compliance Head-1 also noted that the “[f]ees earned are very substantial and if lost will significantly impact the business (probably terminate the business).”

63. The London Compliance Officer therefore immediately recognized the Olympus-related structure could “present an unacceptable regulatory risk to the Commerzbank Group.” On or about September 18, 2008, the London Compliance Officer met with the COSEA Managing Director to discuss the Olympus-related structure. According to the London Compliance Officer’s notes of that meeting, the COSEA Managing Director explained that he had not received any explanation of the “economic rationale” for the SG Bond structure. The London Compliance Officer said that Commerz might have to terminate the relationship with Olympus if “we can’t get to the bottom of the structure.”

64. The following day, the London Compliance Officer met with CITS Managing Director-2 and others to discuss the Olympus-related structure. In that meeting, CITS Managing Director-2 confirmed basic facts about the arrangement—including its structure, its purported purpose, and the involvement of Chan Ming Fon. According to his notes, the London Compliance Officer “explained that by [the Bank’s] not having visibility into [the structure], CBK [*i.e.*, Commerzbank] is vulnerable if OC [*i.e.*, Olympus], EIL [*i.e.*, Easterside] or any other element in the chain is up to no good.” The London Compliance Officer gave the example of Merrill Lynch’s regulatory fine “for aiding and abetting Sumitomo.” At no point in that meeting, or at any other time, did CITS Managing Director-2 share his concerns about the structure with the London Compliance Officer—the same concerns that he had laid out in a memorandum to the COSEA Managing Director less than a month earlier.

65. After meeting with the COSEA Managing Director and CITS Managing Director-2, the London Compliance Officer indicated in a September 22, 2008 e-mail to the COSEA Managing Director, CITS Managing Director-2, and two Singapore-based compliance officers that he “remain[ed] concerned” about the Olympus-related structures, including, among other

things, (a) the fact that Commerz had no direct contact with Olympus at that point; (b) that there was no verification “of the structure’s ultimate purpose”; and (c) “the structure appears open ended.” The e-mail concluded that the business “must urgently arrange a meeting with Olympus,” and said he was also “concerned that [CITS Managing Director-2] does not ask about the client’s intentions,” noting that the Monetary Authority of Singapore (“MAS”) requires trust companies to monitor their clients’ activities for AML purposes. The London Compliance Officer concluded:

As I mentioned on Friday, apart from checking the source of money we receive, we must also consider how clients use money we handle for them. Do not doubt that we would face both regulatory sanction and bad publicity if we were found to have facilitated illegal share support, insider dealing, evasion of disclosure rules or the commission of any other deception or crime, financial or otherwise.

66. In an e-mail dated only two days later, on September 24, 2008, to the COSEA Managing Director, CITS Managing Director-2, and three Singapore-based compliance officers, the London Compliance Officer noted that a meeting had been arranged with Olympus, but that it was “not due for a month” and asked for it to be moved up. He continued:

I say again that we have to be concerned within reason about what clients do with facilities we provide them and money we remit on their behalf.

I’m afraid that regulators will not accept the defense that all business relations were established before the effective date of [a particular MAS notice] and that they escape the due diligence mandated by the Notice. Neither will they accept the defense that CITS only provided certain kinds of services and is somehow entitled to shut its eyes to certain parts of a complex structure and/or unusual transactions.

During our meeting on Friday, however, you said that you have not asked questions about clients’ intentions as you felt you were at less risk by not knowing. I’m afraid such an attitude is inappropriate, especially from someone in a senior position. . . .

You mentioned that Olympus is well-established and is a listed multi-national corporation which gives comfort that the source of funds was legitimate. Remember, though, that many large and apparently reputable companies have run into severe legal and regulatory problems, sometimes dragging their bankers into the mire.

The London Compliance Officer's e-mail then listed a number of high-profile companies and their bankers that had been sanctioned or fined.

67. At about the same time, the London Compliance Officer e-mailed Commerz's Global Head of Compliance to relay the same concerns. His e-mail, for example, noted that CITS Managing Director-2 "said that he did not typically ask questions of clients as he felt he was at less risk by not knowing," and that the COSEA Managing Director "said he did not understand, so I repeated that it is unacceptable for senior managers to turn blind eyes or otherwise remain ignorant."

68. In a report dated October 16, 2008, to the Global Head of Compliance, the London Compliance Officer delivered his review of CITS and COSEA's accounts. Among other things, the London Compliance Officer highlighted the Olympus-related structures, and criticized COSEA and CITS business people for their "delay in meeting officers of the Olympus Corporation to discuss directly the purpose of the complex structure involving Easterside Investments Limited."

69. In another e-mail to the Global Head of Compliance, dated November 23, 2008, the London Compliance Officer noted that the "putative purpose" of the Olympus-related structures was to "disguise" Olympus's stake in the SPV, and continued that "[t]he structure is complex and could be used to disguise many other things," such as "avoiding anti-monopoly laws," "supporting OC's share price," or "avoiding disclosure rules." The London Compliance Officer also noted that the proffered reason for the structure—to allow Olympus to secretly make

strategic investments into competitors in the market for endoscopic products—was contrary to a number of statements in Olympus’s annual reports. For example, Olympus had represented to CITS employees that the purpose of the SPV was to increase Olympus’s market share in the endoscopic devices market. But Olympus’s annual report, as the London Compliance Officer noted, indicated that Olympus already held an “overwhelming 80% share of the world market” for endoscopic devices, and that rather than seeking to increase market share, Olympus sought a “departure from an endoscopic-dependent operation.” The London Compliance Officer also observed that there had still not been a meeting with representatives of Olympus, and that the meeting had been pushed off until December 2008.

70. According to CITS documents, the COSEA Managing Director and CITS Managing Director-2 met with senior Olympus officials (including two who subsequently pleaded guilty) and Chan Ming Fon in Tokyo on or about December 4, 2008. According to a report of that meeting written by CITS Managing Director-2, the COSEA Managing Director asked to “understand more about the structure, which originates from as far back as 1996.” The report stated “[a]ll our questions were answered friendly and straightforwardly. The representations made by senior board members in the meeting were very convincing.” An Olympus representative reportedly confirmed that the purpose of the structure was to make secret investments in competitors, “but only off balance sheet.” The notes reflect that “we will only be able to obtain verbal positive confirmation as given in the meeting for the time being”—that is, there was no other verification of the purpose of the structures. The report concluded that “we are confident with this business. The impact on CITS income is substantial. Nonetheless, the board of CITS should discuss the suitability for this kind of business for a trust company and a private bank going forward.”

71. By that point, however, the London Compliance Officer had left Singapore; approximately four months later, he was installed as the head of compliance for Commerz New York. He noted in an e-mail to other Commerz Asia compliance personnel—written in early January 2009, after he had left Singapore but before arriving in the United States—that at a dinner before he left Singapore with the Asia Compliance Head-1 and a CITS director (the “Statutory Director”), the Statutory Director had again pressed on why the Olympus structure was “suspicious and why it was CBK’s [*i.e.*, Commerz’s] duty to look below the surface.”

72. When he received a copy of the December 4, 2008 meeting notes by CITS Managing Director-2, the London Compliance Officer remarked, “Everyone is on notice. I’m not sure there’s much more we can do unless new information comes to hand.” In interviews with federal investigators, the London Compliance Officer asserted he meant that, although the meeting notes were not thorough enough and did not address all of his questions, the relevant people—including the relevant business heads and the incoming Head of Compliance in Asia (the “Asia Compliance Officer”), who were copied on the e-mail—had all of the information necessary to act, and that it was now their responsibility, as the London Compliance Officer had already left Singapore by the time he received the meeting notes.

73. Upon arriving in New York in or about April 2009 and assuming his new job as head of compliance for Commerz New York, the London Compliance Officer was contacted by a senior compliance officer in Singapore, who asked about the Olympus structure, noting that “[i]t seems a very complicated structure without any economical rationale.” The Singapore compliance officer asked a number of questions, including “Did you feel comfortable in the end?” The London Compliance Officer responded that he could not recall all of the details and that he had been occupied with a very sensitive employee disciplinary issue concerning the

COSEA Managing Director (who was ultimately forced to resign) that “dominated” his attention at the end of his tenure in Singapore. Nonetheless, the London Compliance Officer explained:

I was never comfortable with the structure or CMF’s [*i.e.*, Chan Ming Fon’s] involvement (I think [CITS Managing Director-2] relied on him far too much), but acting on the basis that one is innocent until proven guilty and I had no proof of wrongdoing, it was left on a watching brief which I suppose is where you come in.

74. The London Compliance Officer, the CITS Managing Director-2, the Asia Compliance Head-1, and the Singapore compliance officer who followed up in April 2009 were not the only people at Commerz to be suspicious of the Olympus-related structure. Rather, other business and compliance personnel in Singapore had articulated similar concerns questioning “the economic rationale for the transaction” as well as whether “CDD” (customer due diligence) had been performed on the client (including one proposed Olympus transaction that, although very similar to the SG Bond structure, Commerz eventually declined as “too unusual for my liking”). One compliance officer pointed to an AML notice published by the MAS, which required trust companies like CITS to “pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.” Another compliance official in Singapore responded that Commerz representatives should meet with multiple Olympus officials “to ensure that in case there is any fraud (I am not saying there is), this should flush it out.” And, as noted above, another described the Olympus-related structure as “a very complicated structure without any economical rationale.”

75. Between 2005 and 2010, CITS and COSEA earned at least approximately \$3 million combined for their roles in the Olympus structure.

Suspicious at Commerz New York in 2010

76. Notwithstanding the concerns articulated by the London Compliance Officer, the Asia Compliance Head-1, and others, no negative information about Olympus or any related entity was ever transmitted to Commerz New York, either directly or through Frankfurt, even as more than \$1.6 billion in Olympus-related transactions were being routed through Commerz New York between 1999 and 2010. In early 2010, two Olympus-related transactions “alerted” in Commerz New York’s transaction monitoring software as a result of the introduction by Commerz of more sophisticated transaction-monitoring software and the additional information provided by the new SWIFT messaging format. Specifically, in March 2010—while the London Compliance Officer was still located at Commerz New York, but had been demoted and removed from his position as head of compliance—two wires in the amount of approximately \$455 million and \$67 million from GPA Investment Limited to Creative Dragons SPC-Sub Fund E—both entities involved in the Olympus scheme—alerted in New York. The \$455 million wire was the single highest value transaction by any COSEA client in 2010.

77. AML compliance officers in New York sent a request for information directly to Singapore, as well as to a dedicated mailbox for information requests in Frankfurt, asking for information about the identities of the ultimate originator and recipient of the transactions; the main business of the parties; and the purpose of the transactions.

78. Meanwhile, compliance officers in Singapore had previously identified the same two Olympus-related wires as potentially suspicious. After looking into the transactions, a CITS employee in Singapore, in an e-mail that also copied the Asia Compliance Officer, CITS Managing Director-2, and the head of compliance for Singapore, all of whom were well aware of the concerns about the Olympus-related transactions—explained that the two proposed wires were related to Olympus.

79. In response to Commerz New York's request for information, however, compliance personnel at Commerz Singapore did not relay any of the concerns about the Olympus-sponsored structures and transactions. Instead, the only response to the request for information came in the form of a brief e-mail on or about April 20, 2010:

GPA Investments Ltd. ist [sic] a Caymen [sic] Islands SPV, Creative Dragons SPC-Sub Fund E 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 investment to be reinvested.

Based on this 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.

Olympus-Related Wires Through New York

80. As a result of Commerz's participation in the Olympus-related structure, and the failure to communicate information and concerns about the structure to Commerz New York, at least the following transactions flowed through Commerz New York in furtherance of the Olympus accounting fraud.

Approximate Date	Beneficiary	Amount
6/3/1999	Chan Ming Fon	\$136,584.00
10/6/1999	Commerzbank	\$201,000,000.00
10/8/1999	Twenty-First Century	\$199,813,084.11
10/14/1999	Commerzbank	\$15.00
12/27/1999	Commerzbank	\$101,000,000.00
12/28/1999	Twenty-First Century	\$99,950,000.00
12/29/1999	Commerzbank	\$15.00
3/17/2000	Sumitomo	\$109,479.96
4/24/2000	Spectech	\$755.00
9/25/2000	Sumitomo	\$64,423.41
9/29/2000	Hillmore	\$13,212,222.22
9/29/2000	CITS	\$20,022.14
10/10/2000	Hillmore	\$100,000,000.00

Approximate Date	Beneficiary	Amount
10/10/2000	Hillmore	\$100,000,000.00
10/11/2000	Hillmore	\$38,008.28
10/11/2000	Sumitomo	\$212,266,636.67
12/14/2000	Hillmore	\$7,017,719.30
12/27/2000	Sumitomo	\$6,590,277.78
2/26/2001	Hillmore	\$101,165,777.78
2/26/2001	CITS	\$1,852.11
2/27/2001	Sumitomo	\$2,093,418.32
2/27/2001	Sumitomo	\$101,115,970.00
6/27/2008	GPA Investments Ltd.	\$68,600,000.00
6/30/2008	GPA Investments Ltd.	\$51,000,000.00
7/3/2008	GPA Investments Ltd.	\$10,000,000.00
9/25/2008	HSBC	\$650.00
8/18/2009	International Commercial Bank	\$500,000.00
11/06/2009	Standard Chartered	\$5,000.00
12/14/2009		\$100,000
3/31/2010	Creative Dragons	\$455,000,000
3/31/2010	Creative Dragons	\$66,997,457.63
4/7/2010	Creative Dragons	\$100,000,000
4/8/2010	Creative Dragons	\$150,000
4/16/2010	Creative Dragons	\$12,910.89
4/28/2010	VAP Communications	\$6,500,000.00
5/5/2010	Dragons Asset Mgmt	\$3,000,000.00
6/16/2010	Dragons Asset Mgmt	\$3,000,000.00
6/23/2010	Chan Ming Fon	\$1,000,000.00
8/17/2010	Conyers Dill	\$430.98
	Total	\$1,648,246,073.91

Commerz New York Failed to Adequately Monitor Correspondent Banking Transactions

81. In or about October 2011, the Olympus accounting fraud was revealed, precipitating the filing of SARs in the United States and Suspicious Transaction Reports in Singapore (which are filed based on a different standard than SARs). Prior to the revelation of the fraud, however, no negative information about Olympus—indeed, no indication that the transactions through the New York branch even involved Olympus—was communicated to Commerz New York. And the Singapore branch, although suspicious of the Olympus transactions, had filed only a single STR in July 2010, related to one or more payments to Chan Ming Fon.

82. Although the routing through Commerz New York of more than \$1.6 billion in transactions that Bank officials suspected to be part of a structure that had no “economic rationale” and that could be used to disguise other illegalities—and thus was reportable under the BSA—is a stark example of a compliance deficiency, Commerz New York was repeatedly criticized for its AML compliance deficiencies by Commerz’s own internal audit function and its regulators in the United States. Those criticisms persisted over a number of years. In turn, Commerz New York’s compliance department criticized Commerz Frankfurt and other branches for failing to provide the information it needed to comply with the BSA.

Commerz New York Raised AML Compliance Concerns with Frankfurt

83. The same person served as Commerz’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 the home office in Frankfurt.

84. In interviews with federal investigators, the BSA Officer noted that until late 2006, there was no global policy at Commerz of maintaining KYC materials for the customers of the correspondent banking business (*i.e.*, the customers of Commerz branches and affiliates). Although the BSA does not require a financial institution to conduct due diligence of its customer’s customers, it is still 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, as described above, Commerz New York failed to do—and by sending requests for further information to the correspondent bank when potentially suspicious transactions are detected.

85. The BSA Officer explained, however, that she observed that relationship managers outside of Commerz New York did not maintain KYC files consistent with U.S. requirements, and that Commerz New York frequently had difficulties getting responses to

requests for information that were generated in connection with automated “alerts.” According to another New York-based compliance officer responsible for AML transaction monitoring, because requests for information went unanswered for as much as eight months without SARs being filed, alerts were often closed out 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. The BSA Officer further observed that at times certain business units in Frankfurt resisted the independent judgments of AML personnel in New York, a problem that the BSA Officer and other New York based compliance personnel raised with successive Global Heads of Compliance. The BSA Officer further observed that Commerz Frankfurt felt that Commerz New York was “crying wolf” when it raised compliance issues.

86. For example, in an e-mail dated June 24, 2010, a New York based compliance officer who had primary responsibility for automated transaction monitoring wrote in an e-mail to the BSA Officer and the Asia Compliance Officer (who had recently assumed the position of Head of Compliance in New York) 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 Asia Compliance Officer forwarded the e-mail to the Bank’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.

87. After the BSA Officer realized that a transaction with a so-called Specially Designated National (*i.e.*, a person or entity subject to U.S. sanctions) was processed in 2009 as a result of incomplete or incorrect information received from Commerz Frankfurt about the correspondent banking relationship, the BSA Officer determined to do more due diligence in New York. However, Commerz New York received resistance from Frankfurt in implementing that project.

88. Similarly, according to both the BSA Officer and another New York compliance officer, in or about 2009, Commerz New York added a particular money exchanger to an AML filter in order to detect and block any transactions involving that correspondent banking customer due to a history of suspicious activity. Although Commerz Frankfurt, acting at the direction of the Global Head of Compliance, ultimately agreed to close accounts with and filter all money exchanger customers, Commerz Frankfurt initially instructed New York to remove the client from the filter, and criticized the Commerz New York AML compliance employees for acting without consulting the business in Frankfurt. The same thing happened, according to the BSA Officer, with a Kabul-based correspondent banking customer that had engaged in apparently suspicious activities. Although the customer was ultimately placed on the filter, Commerz Frankfurt, acting through certain employees, initially instructed the BSA Officer, the person at Commerz responsible for the Bank's compliance with U.S. law, that she—and Commerz New York—did not have the ability to put any client into a filter without the approval of Frankfurt (a situation that was rectified in 2011 by the creation of a joint committee chartered with determining which clients should be added to these blocking filters). The Global Head of

Compliance told federal investigators that when Commerz New York blocked transactions with the money exchanger, there was significant pushback from the business in Frankfurt. In fact, the Global Head of Compliance cited this incident—in which the U.S.-based BSA Officer blocked suspicious transactions in accordance with the BSA—as one of the reasons that the London Compliance Officer was ultimately fired. According to the Global Head of Compliance, Commerz New York needed to respect the “process” for such actions, including apprising the Frankfurt-based business and Group Compliance, because the abrupt termination of the client’s account was disruptive to the business.

89. Business people within Commerz New York were also perceived as indifferent to compliance matters. For example, one compliance officer told federal investigators that he raised a compliance issue related to the correspondent banking business with a senior executive of the North American business, who “flipped out” and said, in substance, why did you tell this to me and make it my problem? The senior executive also asked why the Bank should care what a client was doing with its money.

*Internal Audit Found Numerous Deficiencies with Commerz New York's
AML Compliance Program*

90. At the time that Commerz acquired Dresdner Bank in late 2008, Dresdner Bank was operating under a Cease and Desist Order issued by the Board of Governors of the Federal Reserve and the New York State Banking Department related to BSA/AML compliance deficiencies in Dresdner’s correspondent banking and dollar clearing businesses. Commerz was able to convince the Federal Reserve to lift that order upon completion of the merger, and reported regularly to the Federal Reserve on the progress of the banks’ integrations.

91. In or about September and October 2009, Commerz Group Audit conducted a full scope review of Commerz New York’s AML compliance program in the wake of the Dresdner

merger and integration. The audit report, dated November 2009—which was distributed to Commerz’s senior leadership, including to certain members of Commerz’s Board of Directors, the Global Head of Compliance, the New York-based CEO and COO of Commerz’s North American Business, and its BSA Officer—concluded that the overall assessment of Commerz New York’s AML compliance program was “fair,” which equated to a score of three on a five-point scale. The audit report had numerous findings related to the BSA/AML compliance program, such as:

- a. Commerz New York had no process or procedure in place for conducting enhanced due diligence and enhanced account activity monitoring (in part, because prior to the acquisition of Dresdner, Commerz New York did not consider itself to have high risk clients), which the audit report noted was a “high risk” deficiency that “present[s] a higher money laundering or terrorist financing risk [and] exposes the Bank to regulatory risks.”
- b. In its KYC process, Commerz New York only assessed demand deposit accounts for enhanced due diligence, even though the Bank maintained other sorts of client relationships.
- c. “[N]o enhanced account activity [was] performed on the following customer-types: Clients classified as high-risk in the Customer Risk Rating Tool . . . [and] Foreign financial institutions operating in high-risk jurisdictions.”
- d. Commerz New York maintained a backlog of more than 1,600 uninvestigated AML alerts, which the audit report noted was another high-risk deficiency that created the “[p]ossibility of suspicious activities being undetected.”
- e. The information upon which AML investigations were based “did not always provide for a clear picture of the final outcome of the investigation.”

92. According to numerous Commerz New York compliance officials, the 2009 AML audit report of Commerz New York was amongst the most negative internal audit reports in memory. To address the audit findings, which were shared with its regulators, Commerz engaged in broad remediation efforts, including retaining independent consultants. Ultimately,

all of the audit findings were remediated and, after undergoing testing by the internal audit department, closed out by mid-2011; all findings deemed high risk were closed out by the end of August 2010.

Commerz's Regulators Repeatedly Warned the Bank About AML Compliance Issues

93. In February and March 2013, officials from FRBNY and the New York State Department of Financial Services ("DFS") conducted an examination of Commerz New York's BSA/AML compliance program. The regulators determined that "the branch's BSA/AML compliance program remains inadequate," and that "management has failed to implement internal controls to appropriately identify, mitigate, and manage the BSA/AML risks associated with the branch's foreign correspondent banking business." The regulators noted that these findings were "similar" to ones identified during a 2011 FRBNY examination of Commerz's so-called wholesale banknotes business.

94. Among other things, the regulators criticized Commerz New York for failing to "conduct[] appropriate due diligence of the branch's foreign correspondent relationships," and noted that "[t]he exam also identified violations of BSA/AML laws and regulations that were the result of systemic internal control weaknesses."

95. With respect to systemic weakness at Commerz New York, the regulators pointed to the fact that "[t]he branch has not yet developed sufficient risk-based monitoring processes for MT 202 transactions," *i.e.*, transactions processed through the new SWIFT messaging format introduced in 2009, which were not reviewed for suspicious activity at all. "Instead, the MT 202 reviews were limited to key word searches for phrases indicative of cover payments"—a result that might suffice to detect transactions with entities subject to U.S. sanctions, but which could not otherwise detect suspicious activity.

96. In an interview with federal investigators, a Commerz New York compliance employee involved in establishing the thresholds used by the monitoring software in effect until 2010, told federal investigators that while the goal of the threshold setting process was to identify suspicious transactions, and to exclude irrelevant transactions, the threshold floors were driven by the output of alerts. That is, the threshold floors were set based on a desire not to generate “too many alerts.” According to another compliance officer during an interview with federal investigators, the then-Head of Compliance for the New York branch required a weekly update on the number of alerts and, in 2011, asked him to change the thresholds in the automated system to reduce the number of alerts generated. The compliance officer reported that he refused to do so.

97. An outside consultant had originally assisted in setting the transaction monitoring rules and thresholds, but the thresholds were subsequently adjusted (prior to the 2013 FRBNY/DFS examination) in an effort to manage the alert volume. The regulators also noted that Commerz New York’s transaction monitoring program had been calibrated in certain ways that seemed to defy explanation, and for which there was no documentation. For example, the threshold for excessive daily funds transfers for a single account was set at \$2 billion, when the average transaction levels were less than \$1 million. In an interview with federal investigators, however, the BSA Officer explained that the specific threshold that had been criticized by the regulators—the \$2 billion one-day threshold—was not the result of attempting to manage the number of alerts. Rather, she explained that an outside consultant had recommended removing that threshold altogether because it was redundant of other rules, but that the AML staff had instead decided to retain the threshold but to set it especially high. As the regulators noted, there was no contemporaneous documentation of this explanation.

98. The regulators also specifically identified deficiencies with Commerz Frankfurt's role in BSA/AML compliance, including the quality of enhanced due diligence files for head office and global branches' customers (which was "inadequate" and did "not address the intended use of the correspondent relationship"), and Frankfurt's response to requests for information from the New York branch. Specifically, the regulators wrote that their qualitative testing "identified instances where [] requests for further information had been insufficiently evaluated along with occurrences of red flags within transaction details that had not been further investigated."

99. As the regulators noted, Commerz New York had previously received a negative examination report in connection with BSA/AML compliance deficiencies in its wholesale banknotes business. Specifically, FRBNY examiners determined that Commerz New York had numerous deficiencies in its BSA/AML compliance program related to the banknotes business, including that Commerz New York failed to perform adequate customer due diligence on the correspondent account maintained for Commerz Frankfurt or to risk-rate the banknotes business. That examination resulted, in or about June 2012, in a written order on consent between FRBNY and Commerz that required Commerz to remediate its BSA/AML deficiencies and to make regular reports to FRBNY. Among other things, the 2012 written order required Commerz to develop an AML compliance program that included "comprehensive customer due diligence and enhanced due diligence policies, procedures, and practices for its customers, including, but not limited to, Commerzbank AG," *i.e.*, Commerz Frankfurt.

100. The regulators noted a similar, but broader deficiency in 2013, observing that the Bank had still failed to conduct adequate enhanced due diligence on the head office (*i.e.*, Frankfurt) and global branches and affiliates in its correspondent banking business. Among

other things, the regulators found that the “customer files do not address the intended use of the correspondent relationship, the expected volumes and frequency of activity arising from transactions, the locations and types of customers, etc.” Moreover, the regulators found “[s]imilar weaknesses . . . for non-affiliated customer files.”

101. The 2013 correspondent banking examination likewise resulted in an enforcement action, which Commerz resolved by consenting, in or about October 2013, to a Cease and Desist Order. Under the Order, Commerz New York is required to further remediate its BSA/AML deficiencies and to make regular reports to FRBNY. Among other things, the Bank is required to implement “an acceptable customer due diligence program,” including, at a minimum, “[p]olicies, procedures, and controls to ensure that the [New York] Branch collects, analyzes, and retains complete and accurate customer information for all account holders, including but not limited to, affiliates.

ATTACHMENT C

[CERTIFICATE OF CORPORATE RESOLUTIONS –
IN A FORM TO BE PROVIDED BY THE COMPANY]

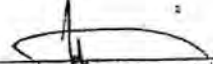
COMPANY OFFICERS' CERTIFICATE

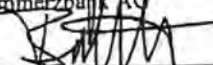
We have read this Agreement and carefully reviewed every part of it with outside counsel for Commerzbank AG and Commerzbank (New York Branch) (collectively, the "Company"). We understand the terms of this Agreement and the Company voluntarily agrees to each of its terms. Before signing this Agreement on behalf of the Company, we consulted outside counsel for the Company. Counsel fully advised us of the rights of the Company, of possible defenses, of the Sentencing Guidelines' provisions, and of the consequences of entering into this Agreement.

We have carefully reviewed the terms of this Agreement with the Managing Board of the Company. We have advised and caused outside counsel for the Company to inform and advise the Managing Board of the Company fully of the rights of the Company, of possible defenses, of the Sentencing Guidelines' provisions, and of the consequences of entering into the Agreement.

No promises or inducements have been made other than those contained in this Agreement. Furthermore, no one has threatened or forced us, or to our knowledge any person authorizing this Agreement on behalf of the Company, in any way to enter into this Agreement. We are also satisfied with outside counsel's representation in this matter. We certify that we are respectively, the General Counsel and the Managing Director - Head of Legal North America for the Company and that we have been duly authorized by the Company to execute this Agreement on behalf of the Company.

Date: April 11, 2015

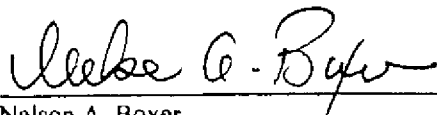
By: 
Günter Huggler, General Counsel
Commerzbank AG

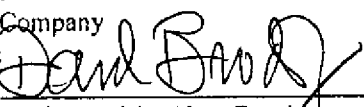
By: 
Armin Barthel, Managing Director - Head of
Legal North America
Commerzbank (New York Branch)

CERTIFICATE OF COUNSEL

We are counsel for Commerzbank AG and Commerzbank (New York Branch) (collectively, the "Company") in the matter covered by this Agreement. In connection with such representation, we have examined relevant Company documents and have discussed the terms of this Agreement with the Managing Board of the Company. Based on our review of the foregoing materials and discussions, and based upon representations to us regarding the laws of Germany, we are of the opinion that the representative of the Company has been duly authorized to enter into this Agreement on behalf of the Company and that this Agreement has been duly and validly authorized, executed, and delivered on behalf of the Company and is a valid and binding obligation of the Company. Further, we have carefully reviewed the terms of this Agreement with the Managing Board of the Company. We have fully advised them of the rights of the Company, of possible defenses, of the Sentencing Guidelines' provisions and of the consequences of entering into this Agreement. To our knowledge, the decision of the Company to enter into this Agreement, based on the authorization of the Managing Board of the Company, is an informed and voluntary one.

Date: 3-11-15

By: 
Nelson A. Boxer
Petrillo Klein & Boxer LLP Counsel for the
Company

By: 
David Brodsky / Lev Dassin
Cleary Gottlieb Steen & Hamilton LLP
Counsel for the Company

ATTACHMENT D

[Sanctions Civil Forfeiture Complaint]

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA)	
)	
)	
Plaintiff,)	
v.)	Civil Action No.
)	
\$92,000,000 IN UNITED STATES CURRENCY BELONGING TO COMMERZBANK AG)	
)	
Defendant.)	

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, plaintiff the United States of America (the "Government"), by and through the United States Attorney for the District of Columbia and the Department of Justice, Criminal Division, Asset Forfeiture and Money Laundering Section, pursuant to Title 18, United States Code, Section 981(a)(1)(A) to bring this verified complaint for forfeiture in a civil action *in rem* against \$92,000,000 in U.S. currency belonging to Commerzbank AG ("Commerz").

NATURE OF ACTION AND THE DEFENDANT *IN REM*

1. This civil action *in rem* is brought against the defendant property to forfeit it to the United States as authorized by 18 U.S.C. § 981(a)(1)(A). The defendant property is \$92,000,000 in U.S. currency belonging to Commerz transferred to the United States Marshals Service by Commerz in conjunction with a Deferred Prosecution Agreement ("DPA") entered into by the United States and Commerz.

2. By this complaint, the United States seeks forfeiture of all right, title, and interest in the defendant property, which Commerz has agreed is forfeitable to the United States as a result of its conspiracy to transmit or transfer funds from a place in the United States to or

through a place outside the United States or to a place in the United States from or through a place outside the United States, in violation of 18 U.S.C. §§ 1956(a)(2), 1956(h), with the intent to promote the carrying on of a conspiracy to violate the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706, in violation of 18 U.S.C. § 371.

3. Commerz has agreed that the facts contained in the Information and in the Statement of Facts filed with the DPA are sufficient to establish that this defendant property is subject to civil forfeiture to the United States.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.

5. Venue is proper within this judicial district pursuant to 28 U.S.C. §§ 1355(b) and 1395(b) because the defendant property is located within the District of Columbia.

STATEMENT OF FACTS

6. At all times relevant to this Complaint, Commerz had its principal place of business in Frankfurt, Germany. Commerz conducts business in Europe, North America, South America, Asia, Africa, and Australia. Since 1967, Commerz has been licensed to operate a foreign bank branch in New York, New York (the "Branch"). The Branch provides U.S. Dollar ("USD") clearing for international wire payments and provides banking services to German companies, subsidiaries of German companies located in the United States, and U.S. companies.

7. As set out in more detail in the Statement of Facts, attached as exhibit A and incorporated herein by reference, IEEPA 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 this authority, Presidents have imposed sanctions on, among other countries, Iran and Sudan.

8. Beginning in or about January 2002 and ending in or about December 2008, Commerz violated U.S. law by assisting clients in evading U.S. sanctions, including those applicable to Iran and Sudan. Specifically, Commerz sent payments involving sanctioned entities or entities affiliated with sanctioned countries through the Branch and other U.S. financial institutions, as part of a conspiracy to violate IEEPA. Commerz knowingly and willfully concealed from the Branch, other U.S. financial institutions, and regulators the sanctioned entities' connection to these transactions, which caused false information to be recorded in business records of the Branch. Consequently, U.S. financial institutions processed transactions that should have been rejected, blocked, or stopped for investigation.

9. More specifically, employees of Commerz: (i) sent payments from Frankfurt on behalf of sanctioned clients without reference to the payments' origin; (ii) eliminated payment data that would have revealed the involvement of sanctioned entities; (iii) directed an Iranian client to transfer payments in the name of its subsidiary companies to mask the Iranian client's involvement; (iv) issued checks to an Iranian client that showed a European-rather than Iranian-address; and (v) used alternative payment methods to conceal the involvement of sanctioned entities.

10. The conspiracy to conceal transactions involving sanctioned entities from the Branch allowed the unlawful payments to go unnoticed.

11. By providing these services to clients that were subject to U.S. sanctions or clients that were doing business with sanctioned entities, Commerz engaged in a conspiracy to violate IEEPA in violation of 18 U.S.C. § 371.

12. Moreover, by providing these services Commerz transmitted or transferred from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of an IEEPA violation, all in violation of 18 U.S.C. §§ 1956(a)(2), 1956(h).

13. Commerz has admitted to transmitting or transferring at least \$92,000,000 of funds derived from a conspiracy to violate IEEPA beginning in or about January 2002 and ending in or about December 2008. The funds involved in these illegal IEEPA transactions passed through Commerz, where they were commingled with other Commerz funds.

14. During that same time frame, the overall assets owned by Commerz was far in excess of \$92,000,000. These funds facilitated and were involved in the illegal transmission and transfer of the \$92,000,000.

15. In March 2015, Commerz transferred \$92,000,000 of its own funds, the defendant property, to the United States Marshals Service.

16. There is a substantial connection between the defendant property and the violation of 18 U.S.C. §§ 1956(a)(2), 1956(h). As Commerz has stipulated in the DPA, the defendant property was involved in the offending transactions. That is, the defendant property is not the \$92,000,000 in funds that violated IEEPA, rather it represents a portion of the property that facilitated those illegal transactions.

CLAIM FOR RELIEF
(18 U.S.C. § 981(a)(1)(A))

17. The Government re-alleges and incorporates by reference paragraphs 1 through 16 as if fully set forth herein.

18. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to forfeiture.

19. “Specified unlawful activity” is defined in 18 U.S.C. § 1956(c)(7) to include, among other things, offenses related to violations of IEEPA.

20. As a result, the defendant property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) as property involved in a violation of 18 U.S.C. §§ 1956(a)(2), 1956(h).

REQUEST FOR RELIEF

WHEREFORE, the plaintiff United States of America prays that process issue to enforce the forfeiture of the *in rem* defendant-property; that, pursuant to law, notice be provided to all interested parties to appear and show cause why the forfeiture should not be decreed and the defendant property be condemned as forfeited to the United States of America; and for such other and further relief as this Court may deem just, necessary and proper, together with the costs and disbursements of this action.

Respectfully submitted,

RONALD C. MACHEN JR.
D.C. Bar No. 447889
United States Attorney

Date: 3/12/2015

BY: /s/ Zia M. Faruqui
Zia Faruqui, D.C. Bar No. 494990
Matt Graves, D.C. Bar No. 481052
Maia Miller, VA Bar No. 73221
Assistant United States Attorneys
555 Fourth Street, N.W., Fourth Floor
Washington, D.C. 20530
(202) 252-7117 (Faruqui)
(202) 252-7762 (Graves)
(202) 252-6737 (Miller)
zia.faruqui@usdoj.gov
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

Date: 3/12/2015

BY: /s/ Sarah Devlin
SARAH DEVLIN
PAM HICKS
Trial Attorneys
Asset Forfeiture and Money Laundering Section

Counsel for Plaintiff United States

VERIFICATION

I, John Matala, a Special Agent with the Internal Revenue Service, Criminal Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement agents and that everything represented herein is true and correct.

Executed on this 11th day of March 2015.

/s/ John Matala _____
John Matala
Special Agent
Internal Revenue Service, Criminal Investigation

ATTACHMENT E

[BSA/AML Civil Forfeiture Complaint]

PREET BHARARA
United States Attorney for the
Southern District of New York
By: BONNIE JONAS
SHARON COHEN LEVIN
Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007
Tel. (212) 637-2472/1060

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	X	
	:	
UNITED STATES OF AMERICA	:	<u>VERIFIED CIVIL COMPLAINT</u>
	:	
-v-	:	15 Civ.
	:	
\$300,000,000 IN UNITED STATES CURRENCY,	:	
	:	
Defendant- <u>in-rem</u> .	:	
-----	X	

Plaintiff United States of America, by its attorney Preet Bharara, United States Attorney for the Southern District of New York, for its verified complaint, alleges, upon information and belief, as follows:

I. JURISDICTION AND VENUE

1. This action is brought pursuant to Title 18, United States Code, Section 981(a)(1)(C) by the United States of America seeking the forfeiture of \$300,000,000 in United States currency (the "Defendant Funds" or the "defendant-in-rem").

2. This Court has jurisdiction pursuant to Title 28, United States Code, Section 1355.

3. Venue is proper under Title 28, United States Code, Section 1355(b)(1)(A) because certain actions and omissions giving rise to forfeiture took place in the Southern District of New York and pursuant to Title 28, United States Code, Section 1395 because the defendant-in-rem has been transferred to the Southern District of New York.

4. The Defendant Funds are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C).

5. Upon entry of a final order forfeiting the Defendant Funds to the United States, the Government intends to distribute the funds to victims of the fraud, consistent with the applicable Department of Justice regulations, through the remission process. *See* Title 21, United States Code, Section 853(i)(1), Title 18, United States Code, Section 981(e)(6), and Title 28, Code of Federal Regulations, Part 9.

II. FACTUAL ALLEGATIONS

6. From at least in or about 2008, and continuing until 2013, the New York branch of Commerzbank AG (“Commerz New York”), acting through certain employees located in New York, violated the BSA and its implementing regulations. Specifically, Commerz New York failed to maintain adequate policies, procedures, and practices to ensure their compliance with U.S. law, including their obligations to detect and report suspicious transaction activity. As a result of the willful failure of Commerz New York to comply with U.S. law, a multi-billion dollar securities fraud was operated through Commerz New York and other reportable transactions under U.S. law were never detected.

7. Commerz New York's AML program allowed the proceeds of fraud and other suspicious transactions to be processed through Commerz New York. Specifically, between 1999 and 2010, Commerz New York processed more than \$1.6 billion in transfers orchestrated by Olympus in furtherance of the Olympus accounting fraud.

8. From 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—including its Chairman, an executive vice president, and its general auditor—pleaded guilty in Japan to inflating the company's net worth by approximately \$1.7 billion.

9. As described in greater detail in the attached Statement of Facts, Olympus, through false representations made by Olympus executives, used Commerzbank AG ("Commerz"), through certain branches and affiliates, to perpetrate its fraud. Among other things, the fraud was perpetrated by Olympus through special purpose vehicles, some of which were created by Commerz—including several executives based in Singapore—at Olympus's direction, using funding from Commerz. One of those Singapore-based executives, Chan Ming Fon—who was involved both in creating the Olympus structure in 1999 while at Commerzbank (Southeast Asia) Ltd., and who later on his own managed an Olympus-related entity in 2005-2010 on behalf of which Chan submitted false confirmations to Olympus's auditors—subsequently pleaded guilty in the United States District Court for the Southern District of New York to conspiracy to commit wire fraud.

10. Additionally, 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." 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 Caymen 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 discussed in the attached Statement of Facts.

11. 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 (an Olympus-related entity) had been involved in six transactions through Commerz New York totaling more than \$522 million.

12. 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.

13. As a result of the failure of Commerz's Singapore branch to communicate to Commerz New York the information and concerns about the Olympus-sponsored structures described in the attached Statement of Facts, and Commerz New York's failure to file any suspicious activity reports, more than \$1.6 billion flowed through Commerz New York in furtherance of the Olympus accounting fraud.

III. THE DEFENDANT IN REM

14. On or about March 11, 2015, Commerz and Commerz New York entered into a Deferred Prosecution Agreement with the United States, wherein, inter alia, Commerz agreed to forfeit \$300,000,000, i.e., the Defendant Funds, to the United States. Commerz agrees that the facts contained in the Deferred Prosecution Agreement, with the accompanying BSA/AML Statement of Facts and Information to be filed, establish the Defendant Funds are subject to forfeiture pursuant to United States Code, Section 981(a)(1)(C) and agree that the Defendant Funds represent a substitute res for the proceeds of the Olympus accounting fraud that flowed through Commerz during the course of the Olympus accounting fraud.

15. The Deferred Prosecution Agreement and the accompanying BSA/AML Statement of Facts are attached as Exhibit 1.

IV. CLAIM FOR FORFEITURE

16. Incorporated herein are the allegations contained in paragraphs one through fourteen of this Verified Complaint.

17. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture “[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to...any offense constituting ‘specific unlawful activity’ (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.”

18. “Specified unlawful activity” is defined in Title 18, United States Code, Section 1956(c)(7), and the term includes, among other things, any offense listed under Title 18, United States Code, Section 1961(1). Section 1961(1) lists, among other things, violations of wire fraud (Section 1343) and “fraud in the sale of securities.”

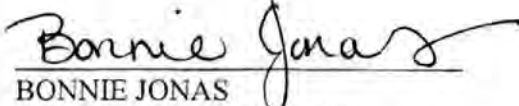
19. Pursuant to Title 18, United States Code, Section 981(a)(2)(A), for purposes of the civil forfeiture statutes, “proceeds” refers to “property of any kind obtained directly or indirectly, as a result of the commission of the offense giving rise to forfeiture, and any property traceable thereto, and is not limited to the net gain or profit realized from the offense.”

20. By reason of the foregoing, the Defendant Funds are subject to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(C) because the Defendant Funds represent a substitute res for the proceeds of the Olympus accounting fraud.

WHEREFORE, plaintiff United States of America prays that process issue to enforce the forfeiture of the defendant-in-rem and that all persons having an interest in the defendant-in-rem be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the defendant-in-rem to the United States of America for disposition according to law, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: New York, New York
March 12, 2015

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the Plaintiff
United States of America

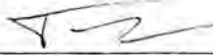
BY: 
BONNIE JONAS
SHARON COHEN LEVIN
Assistant United States Attorneys
One St. Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-2472/1060

VERIFICATION

STATE OF NEW YORK)
COUNTY OF NEW YORK):
SOUTHERN DISTRICT OF NEW YORK)

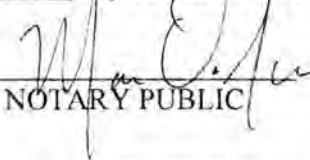
Thomas W. McDonald, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and as such has responsibility for the within action; that he has read the foregoing complaint and knows the contents thereof, and that the same is true to the best of his knowledge, information, and belief.

The sources of deponent's information on the ground of his belief are official records and files of the United States, information obtained directly by the deponent, and information obtained by other law enforcement officials, during an investigation of alleged violations of Title 18, United States Code.



Thomas W. McDonald
Special Agent
Federal Bureau of Investigation

Sworn to before me this
10th day of March 2015



NOTARY PUBLIC

MARCO DASILVA
Notary Public, State of New York
No. 01DA6145603
Qualified in Nassau County
My Commission Expires May 8, 2018