NEW YORK STATE DEPARTMENT
OF FINANCIAL SERVICES

In the Matter of

INTESA SANPAOLO S.p.A.
INTESA SANPAOLO S.p.A. NEW YORK BRANCH

CONSENT ORDER UNDER
NEW YORK BANKING LAW §§ 39 and 44

The New York State Department of Financial Services (the "Department" or "DFS"), Intesa Sanpaolo S.p.A. ("Intesa-Milan"), and Intesa Sanpaolo S.p.A. New York Branch ("Intesa-New York" or the "New York Branch") (together, "Intesa" or the "Bank") stipulate that:

INTRODUCTION

The Culture of Compliance in the Age of Risk

1. Global financial institutions serve as the first line of defense against illegal financial transactions in today's fast-paced, interconnected financial network. Federal and New York law require these institutions to design, implement, and execute policies and systems to prevent and detect illegal financial transactions. The Bank Secrecy Act ("BSA"), for example, requires these institutions to report suspicious transactions (via "Suspicious Activity Reports" or "SARs") to the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN"), enabling law enforcement to conduct investigations that result in the future interdiction of these transactions and, ultimately, prosecution or the blocking of bad actors. The

BSA likewise requires financial institutions to have adequate anti-money laundering ("AML") systems in place.

2. New York law imposes these same requirements on its regulated financial institutions.[1] Specifically, the law obligates financial institutions to devise and implement systems reasonably designed to identify and block suspicious activity and transactions prohibited by law. Each institution is expected to configure a system based on the particular risks faced by the institution, considering such factors as its size, geographical reach, and specific lines of business. Moreover, the institution must employ or engage sufficient numbers of trained compliance professionals to ensure that its systems run properly.

Transaction Monitoring – An Essential Compliance Tool

3. One such system is known as "transaction monitoring." This is the process by which an institution monitors financial transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting. While this process may be carried out manually, larger institutions often employ electronic systems using advanced software to monitor transactions and, in the first instance, screen them even before execution for possible violations of federal sanctions laws.

4. Attention to detail in the operation of these monitoring and filtering systems is essential. A system must be designed to address the specific risks encountered by the institution in conducting its business. Effective transaction monitoring and filtering also necessitates a system that can be adjusted to changes in risk profiles, and which can be audited routinely.

[1] *See, e.g.*, Part 115 of the Superintendent's Regulations (3 NYCRR 115), Part 116 (3 NYCRR 116), Part 416 (3 NYCRR 416) and Part 417 (3 NYCRR 417).

Skilled, adequately-trained staff is also necessary to operate and oversee these systems competently.

5. Ultimate responsibility for the design and implementation of a transaction monitoring system lies at the top echelon of the financial institution. The board of directors and senior management must adequately oversee the compliance, infrastructure, and other personnel that design, implement, operate and (as necessary) modify a transaction monitoring system.

6. In both past investigations and routine examinations, the Department has identified significant shortcomings in transaction monitoring and filtering programs of a number of major financial institutions. The Department found that such deficiencies generally were attributable to a lack of robust governance, oversight, and accountability at senior levels. These findings have resulted in a number of enforcement actions, and have led the Department to issue a new regulation (effective January 1, 2017) governing transaction monitoring and filtering systems. Among other things, the regulation creates an obligation for a covered institution's chief compliance officer (or functional equivalent) to certify compliance with this regulation, thereby encouraging institutions to proactively ensure compliance with existing federal and state anti-money laundering and sanctions requirements. The Department views effective transaction monitoring systems as an essential tool in the battle against illicit transactions and terrorist financing in this age of risk.

Summary of Findings

7. This Consent Order first addresses compliance failures at the New York Branch over the last several years arising from deficiencies in the implementation and oversight of the transaction monitoring system located at the New York Branch.

8. Additionally, the Bank suffered a separate compliance failure in 2005–2006 arising from the processing of thousands of transactions bearing strong indicia of shell company activity or other possible money laundering activity, which were cleared through the New York Branch or other U.S. banks or branches. From 2008 to 2012, the Bank discontinued relationships with approximately 5,400 clients to remediate this compliance failure

9. Further, from approximately 2002 to 2006, Intesa used non-transparent practices to process payments on behalf of Iranian clients and other entities. While these transactions may very well have been legally permissible "U-Turn" transactions under federal law and regulations in effect at the time, they involved non-transparent payment messages. Consequently, the Bank deprived the Department of the opportunity to learn of the true nature of these transactions when carrying out its supervisory responsibilities.

10. The Bank made the decision to discontinue this practice in 2006. In addition, the Bank reached a settlement with the U.S. Treasury Department's Office of Foreign Asset Control ("OFAC") in 2013 in which it paid $2.9 million for apparent violations of federal sanctions laws and regulations related to processing certain U.S. dollar transactions that terminated in the United States for Iranian, Sudanese, and Cuban entities.

FACTUAL FINDINGS

Background on Intesa

11. Intesa is a major international banking institution headquartered in Milan, Italy. The Bank has over 4,000 branches globally. Additionally, it has approximately 1,200 branches belonging to subsidiaries in Central and Eastern Europe, the Middle East, North Africa, Asia, and the United States. The Bank employs more than 90,000 people across the globe.

12. Intesa's financial services businesses include retail lending, wealth management, asset management, and corporate and investment banking. The Bank holds total assets exceeding $761 billion; assets at the New York Branch total approximately $18 billion. It remains one of the top banks in Italy by total assets, and is a key player in the world financial system.

13. The Department supervises and regulates Intesa's New York Branch as a foreign bank branch in New York State. According to the Bank, the New York Branch clears approximately $4 trillion each year through its correspondent banking relationships. This enormous volume of transactions poses significant risks for money laundering and other illicit transactions that need to be properly mitigated by the Bank's leadership.

The 2007 Written Agreement with the Department

14. Following a joint examination by the Department and Federal Reserve Bank of New York ("FRBNY"), the Department (via its predecessor, the Banking Department) and FRBNY commenced a public enforcement action against the Bank and the New York Branch pursuant to a Written Agreement (the "Agreement") dated March 2, 2007. The Agreement sought to address multiple deficiencies identified by the Department in Intesa's BSA/AML compliance.

15. Among other things, the Agreement required important and material improvements in Intesa's BSA/AML compliance, Suspicious Activity Reporting, and Customer Due Diligence efforts. The Agreement also required a limited transaction "look-back" for a six month period in 2006 (the "Initial Look-Back"), to determine the extent of compliance failures at the New York Branch. The Bank hired an independent consultant to assist in its efforts to remediate deficiencies identified in the Written Agreement and to conduct the Initial Look-Back.

The Initial Look-Back was concluded, and a comprehensive written report by the independent consultant was submitted to the Department and FRBNY in 2009.

16. Upon consideration of the results from the Initial Look-Back, the Department required Intesa in December 2013 (the "December 2013 Order") to (1) conduct an expanded look-back for the period of 2005 through 2006, focusing on possible shell company activity first identified during the Initial Look-Back (the "Expanded Look-Back"), and (2) review the existing AML/BSA compliance systems utilized by the New York Branch and make recommendations for correcting any deficiencies.

17. The term "shell company" typically refers to privately-held corporations, limited liability companies (LLCs), and trusts that frequently have no physical presence (other than a post office box), and generate little or no independent economic value. Shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate. Ownership and transactional information on these entities can readily be concealed from regulatory and law enforcement authorities, because most states do not collect or otherwise require disclosure of ownership information at the formation stage or thereafter.[2]

18. Under its December 2013 Order, the Department and the Bank selected a new independent consultant (the "Second Independent Consultant") to (1) perform the Expanded

[2] *See* FinCEN Advisory, *Potential Money Laundering Risks Related to Shell Companies* (FIN-2006-G014, Nov. 9, 2006), at https://www.fincen.gov/resources/statutes-regulations/guidance/potential-money-laundering-risks-related-shell-companies. Indeed, because of concerns about shell company activity, FinCEN recently expanded its efforts to prevent money laundering and terrorist financing by issuing a Geographic Targeting Order that requires title insurance companies to identify natural persons who are behind shell companies that pay all cash for high-end residential real estate in six major metropolitan areas. *See* FinCEN Expands Reach of Real Estate "Geographic Targeting Orders" Beyond Manhattan and Miami (FinCEN July 27, 2016), at https://www.fincen.gov/news/news-releases/fincen-expands-reach-real-estate-geographic-targeting-orders-beyond-manhattan.

Look-Back concerning shell company activity in 2005 through 2006, and (2) conduct the comprehensive review of all existing AML/BSA compliance systems utilized by the New York Branch and make recommendations to correct any deficiencies. The Second Independent Consultant has conducted an investigation since 2014 to further the Department's supervisory and enforcement efforts, and the Second Independent Consultant's investigative efforts have continued to the present.

The Transaction Monitoring System at the New York Branch Is Deficient

19. ***The Bank's System and Governing Policies/Procedures***: The Bank's transaction monitoring system is divided between two electronic programs. The first program – known as "GIFTS-EDD" – employs keywords and algorithms to identify suspicious transactions. When there is a hit on a keyword or when the algorithm is satisfied, the program generates an electronic "alert."[3]

20. An alert may be prompted by such factors as the presence of key terms within a payment message; a relationship to other payments by the same originator or beneficiary; unusual criteria such as round-dollar payments or frequent repetitive payments that appear unrelated to a party's legitimate business purposes; a potential match with persons or entities appearing on lists of persons or entities specifically prohibited from conducting transactions ("specially-designated national" or "SDN" lists); involvement of parties who appear on lists of people who have governmental positions that may subject them to attempts at bribery ("politically-exposed persons" or "PEP" lists); or certain combinations of these indicia.

[3] An alert is not a suspicious transaction in itself. Rather, it is a transaction that contains indicia of potentially suspicious activity and must be investigated to exclude or confirm the existence of suspicious features.

21. The second program – known as "Casetracker" – is a case management system. According to the New York Branch's General Transaction Monitoring Procedures (the "Monitoring Procedures"), each and every alert generated by GIFTS-EDD is supposed to be loaded into Casetracker by compliance personnel.

22. Indeed, for keyword-based alerts, the Monitoring Procedures specifically mandate that each alert be loaded into the case management system even if an alert appears to be a "false positive," that is, a transaction that alerts due to language in a transaction message that is not actually the term or word intended.[4]

23. Once done, New York Branch compliance staff are required to review each alert and decide whether it warrants further investigation or escalation – including the filing of a SAR – or whether it should be cleared and closed. The reviewer must document the determination whether to investigate, escalate, or close, and the factual basis for this decision. Documentation is critical to effective analysis and auditing of transaction monitoring systems.

24. GIFTS-EDD and Casetracker do not interface with each other directly. Accordingly, the New York Branch's written procedures require compliance personnel to load each and every alert generated by GIFTS-EDD into the Casetracker program manually. The compliance staffer is required to create what is essentially a spreadsheet containing all of the alerts generated by each keyword each month, and then load those spreadsheets into Casetracker for review.

25. ***Deviations from the Bank's Policies/Procedures***: The New York Branch's policies and procedures were clear and unambiguous in requiring each alert to be loaded into

[4] For example, if the keyword is "silver," which seeks to identify transactions that reference the precious metal, the system will generate an alert on the term, "Silverstar Plumbing Company." Because that term is not actually the term the system is searching for, this alert would likely be deemed a "false positive."

Casetracker for review. Nonetheless, the New York Branch's designated anti-money laundering compliance officer (the "AML Officer") allowed the staff he supervised to decide, on their own, how they would accomplish this alert transfer from GIFTS-EDD to Casetracker for keyword alerts. The AML Officer reported that he simply left it to individual reviewers to decide which process "works best" for them, without standardization, for keyword alerts.

26. More egregiously, in or about 2012, the AML Officer and his staff began reviewing and "clearing" significant volumes of keyword-based alerts without loading them into Casetracker, as expressly required by written policy. For example, if a staff member believed an alert was a "false positive," based on nothing more than a cursory review of the alert, the staffer would omit the alert from the spreadsheet loaded into Casetracker. As such, it was never subject to any subsequent re-review, investigation, documentation, or internal audit.

27. This unauthorized "clearing" process was executed by compliance staff members and interns – and even the AML Officer himself. While the AML Officer claimed to have provided some guidance to staff on how to carry out this unauthorized clearing process, no formal training on this unauthorized clearing process was ever provided or documented.

28. From sometime in 2012 until at least mid-2014, these alerts were cleared outside of Casetracker without any formal investigation or the creation of reviewable records. This meant that no one at the Bank had the ability to formally re-review the alerts in Casetracker, nor was there an audit trail in Casetracker of any of the thousands of unauthorized clearances of alerts.[5]

---

[5] In or about mid-2014, compliance staff began to create some brief documentation of the unauthorized alert clearing process within the GIFTS-EDD system itself, but it was inadequate because, among other reasons, it was not compliant with express written procedures; it was ad hoc and irregular; and it was kept

29. Moreover, for two months, ***none*** of the keyword-based alerts were migrated from GIFTS-EDD to Casetracker. There is simply no record of these alerts in the case management system, and the Bank could not find any documentation confirming such transfers.

30. Accordingly, in 2014 alone, approximately 10,000 of the keyword-based alerts generated by GIFTS-EDD – approximately 92 percent of the total keywords generated – were never loaded into Casetracker for formal review, either because they were ignored, or were cleared with no formal review or documentation.

31. The unauthorized clearing practice and repeated failure to properly load alerts into Casetracker continued until approximately March 2016, when the Second Independent Consultant discovered it and brought it to the attention of the Department. The Department immediately instructed the Bank to cease this misconduct.

32. The AML Officer subsequently justified the unauthorized clearing practice on the basis that there purportedly was a very high volume of "false positives" being generated by GIFTS-EDD. The AML Officer claimed this unauthorized clearing method was "more efficient" than the procedure prescribed by the New York Branch's written policies. According to the AML Officer, because the Bank allegedly employed a "risk-based approach," this unauthorized process was acceptable, because a risk-based policy meant (at least to him) that "***if you miss one, you miss one.***"

33. In fact, the New York Branch did not track many thousands of alerts. The Independent Consultant determined that, in 2014 alone, approximately 41 percent of the alerts improperly closed through the unauthorized and ad hoc clearing process were not "false

---

in GIFTS-EDD, not in Casetracker, such that anyone who wanted to audit or review these decisions would have had to look in a different system.

positives" but were proper alerts that required further investigation, of which some may have required further escalation.

34. ***Deficiencies in the GIFTS-EDD Rulebook***: In addition to the disregard of the New York Branch's policies and procedures described above, the GIFTS-EDD system itself contained a number of flaws that went undetected by the Bank.

35. First, some keyword alerts had been incorrectly programmed into the software, thereby failing to capture numerous alerts that the Bank intended to identify and review. One example arose when, in writing the script for a particular keyword search, a third-party programmer (apparently inadvertently) added an extra space into the query. This caused the system to search for an incorrect combination of letters and spaces, and for several years the system did not generate one type of important alert.

36. The consequences of this error were material. In 2014 alone, the system generated alerts from this keyword for only 12 transactions; the Independent Consultant's review determined, however, that – if programmed correctly – this search would have generated ***more than 1,400 alerts***.

37. Second, the algorithms designed to conduct searches in GIFTS-EDD contained other programming errors. As one example, algorithms intended to search for certain country-name information were programmed to generate an alert only if the official country name appeared in the transaction message, neglecting to search for commonly-used short forms of the country names. For example, the system searched for "Russian Federation" – but not "Russia"; the system searched for "Libyan Arab Jamahiriya" – but not "Libya."

38. For 2014 alone, the Second Independent Consultant's review determined that, if these algorithms have been programmed correctly, ***at least $9 billion worth of additional transactions*** would have been subject to alerts and review by compliance staff.

39. Third, an algorithm intended to search for three or more transactions within a ten-day period instead only generated an alert when three or more transactions occurred in a single day. This programming error alone caused the ***omission of at least 1,136 alerts*** during 2014 alone.

40. Fourth, certain properly-functioning algorithms nonetheless were applied only to a subset of the transactions intended – rather than the full universe of transactions.

41. These programming errors were compounded by flawed decision-making from compliance personnel. New York compliance staff decided to modify the suite of algorithms employed by GIFTS-EDD based on a mistaken understanding of system operations. Three pattern algorithms running in the program for a period of time, for example, were eliminated based on a mistaken belief they were duplicative of other algorithms also running. These decisions created material gaps in the Bank's transaction surveillance, causing numerous transactions to go unreviewed.

42. ***Failure to Upload Large Numbers of Alerts Into Casetracker***: The collection of human and machine errors described above substantially diminished the effectiveness of the transaction monitoring system. Unfortunately, the deficiencies did not end there.

43. The Independent Consultant discovered that many of the alerts generated by pattern- or list-based algorithms in GIFTS-EDD were never migrated into Casetracker, for reasons not yet apparent.

44. In sum, due to the breakdowns in the transaction monitoring systems at the New York Branch, the Bank failed to review at least 17,000 alerts, totaling approximately $16.6 billion in transactions during 2014 alone (equaling approximately 13% of the alerts that the system was designed to capture). Deficiencies at the New York Branch, however, occurred before then, and continued until at least March 2016, when discovered by the Independent Consultant. Thus, the total number of missed alerts is far larger.

45. ***Breakdown in Audit and Management Oversight***: As noted above, faults in the New York Branch's transaction monitoring system came to light only recently due to the extensive investigation conducted by the Department's Second Independent Consultant.

46. Senior management in New York and at the Head Office in Milan were unaware of such weaknesses, despite the existence of facts that could have led to their discovery. For example, an internal auditor at the New York Branch stated he was aware, through discussions with compliance staff, that some alerts never made it into Casetracker – even though this practice stood against the Bank's written policies.

47. Similarly, in 2014, a compliance manager who conducted a quarterly quality control review of transaction monitoring, learned from compliance staff about the existence of the unauthorized clearance process outside of Casetracker. The compliance manager noted this deviation in a quarterly report, but it was never escalated for higher-level review. This compliance manager's report prompted no further scrutiny or follow-up from senior management, and the practice continued until the Independent Consultant uncovered it two years later.

48. Equally problematic is the fact that Head Office received reports from the New York CCO, as well as the quarterly quality control reports mentioned above. None of the

departures from written policy concerning screening of alerts caught the attention of anyone in New York or Milan charged with overseeing compliance.

49. Poor oversight also led to faulty efforts by compliance staff and their managers in the day-to-day review process. One example: a transaction that cleared through the New York Branch in May 2014 generated an alert because one of the parties to the transaction was a possible match to someone listed as a "politically-exposed person" or "PEP."

50. A "politically-exposed person" is defined as an individual entrusted with a prominent public function. It is recognized that many such persons, due to their position and influence, are in a position that may be abused for the purpose of committing money laundering, bribery, or facilitating terrorist financing.[6]

51. For this reason, a New York Branch compliance staffer investigated the matter to determine whether the identified party was the same individual listed on the PEP list. The investigation revealed that, while the identified party to the transaction was not a politically-exposed person, the party did have known possible links to organized crime.[7]

52. Nonetheless, the analyst "cleared" and closed the alert as non-suspicious, because the alert had only been generated as a potential match for a politically-exposed person.

Shell Company Activity Indicative of Potentially Suspicious Transactions

53. The deficiencies in transaction monitoring were among several AML deficiencies identified by the Second Independent Consultant. The Expanded Look-Back covering the entire 2005–2006 period confirmed the findings of the Initial Look-Back covering a portion of 2006 – namely, that Intesa cleared thousands of transactions through the New York Branch, totaling

[6] *See* Financial Action Task Force, *Politically Exposed Persons*, at 3 (June 2013).

hundreds of millions of dollars, which bore indicia of potentially suspicious activity in relation to shell companies.

54. As noted above, transactions involving "shell companies" may be suspicious. Ownership and transactional information on these entities can be concealed from regulatory and law enforcement authorities, because many jurisdictions do not collect or otherwise require disclosure of ownership information at any point in time. And shell companies are oftentimes located in an off-shore or other jurisdiction separate from the jurisdiction in which the bank holding the account is located.

55. With this and the findings of the Initial Look-Back in mind, the Second Independent Consultant determined that, during the period 2005 through 2006, one of Intesa's subsidiaries (which had been wholly-owned by Intesa since 1999 and was located in Hungary) handled more than 2,500 transactions in relation to potential shell company activity valued at at least $124.4 million. Yet the Bank processed at least $21 million of these transactions through the New York Branch and is unable to show that it took reasonable steps to determine that these transactions were not suspicious at the time that they were processed.

56. The Expanded Look-Back also uncovered examples of suspicious activity involving government agents or other politically-exposed persons, as well as unusual payment patterns, both of which also may be indicative of money laundering, bribery or other illicit conduct.

57. For example, Intesa's Hungarian subsidiary processed a series of transactions in 2005–2006 on behalf of a corporate customer registered in the British Virgin Islands and that

[7] As part of the investigation, the analyst secured a report from a third-party vendor that maintains databases of high-risk individuals and organizations. That report indicated that the party's name returned hits on risk criteria for "organized crime" and "military" relationships.

used a Swiss mailing address – both of which are well-known secrecy jurisdictions. Two individuals who had applied to receive bankcards linked to that customer account were politically-exposed persons connected to the government of Angola. Intesa's corporate accountholder made payments to a beneficiary who was also a well-known public official of the Angolan government, but that beneficiary held accounts at three different banks in three different countries. Intesa processed these transactions without developing information to show that these troubling criteria were not in fact suspicious.

58. Another representative example involved a corporate customer of Intesa's Hong Kong branch, on whose behalf the New York Branch processed transactions in 2005 – 2006 totaling approximately $70 million. The company was controlled by a billionaire businessman of an Asian nation. Many of the payments processed by the New York Branch involved entities controlled by this billionaire owner on both sides of the transaction; many involved shell companies with no obvious business operations; and many involved round-dollar payments to counterparties organized in known secrecy jurisdictions like the British Virgin Islands.

59. There are additional examples involving other Intesa branches. In 2006, Intesa's Luxembourg subsidiary processed one transaction through the New York Branch for a customer registered at a known shell company address in Panama. This shell company address is associated with the Mossack Fonseca law firm. Mossack Fonseca is a Panamanian firm centrally involved in shell company formation around the globe. These shell companies are possibly designed in some instances to skirt banking and tax laws worldwide, including U.S. laws designed to fight money laundering.

60. Suspicious indicia include the fact that the shell company client of Intesa's Luxembourg subsidiary existed only for about 14 months before dissolution; and that the shell

company's transactions included a large round-dollar payment to another apparent shell company doing its banking in Monaco, which was processed through the New York Branch. The Department's investigation determined that the Panamanian shell company was beneficially owned by Italian shipping magnates who were linked, in 2012, to allegations concerning money laundering and tax evasion schemes.

61. Another example concerns a customer of Intesa's Slovakian subsidiary that engaged in apparent "pass-through" activity. In 2005–2006, this customer regularly received payments from one entity and then immediately paid a similar amount to a different entity. In a one-week period, for example, the Intesa customer received three different payments from a company registered in Cyprus that did its banking in Russia. Each time, the Intesa customer immediately paid out a similar amount to a business registered in Panama with a bank account in Latvia. Intesa processed these payments, including through the New York Branch, but cannot show that the New York Branch took reasonable steps to determine that these transactions were not suspicious.

62. The Independent Consultant uncovered at least 6,600 SWIFT messages, totaling at least $319 million, processed by Intesa during 2005–2006 period that bore strong indicia of possible shell company activity. Of this amount, Intesa processed at least $130 million through the New York Branch without appropriate review or investigation.

Non-Transparent Payment Processing

63. Beginning in 2002, payments for Intesa's financial institution clients were processed through Intesa's operations center in Parma, Italy ("Intesa-Parma"). From 2002 to 2006, a special process was used to clear thousands of Iranian transactions through the New York Branch at a time when Iran was subject to OFAC economic sanctions.

64. Certain Iranian transactions, however, were permitted under the U.S. Department of Treasury's "U-Turn General License" in effect at the time. While the transactions subject to this special process at Intesa had the structure of permissible "U-Turn" transactions under U.S. law and regulations in effect at the time, they involved non-transparent payment messages, because they omitted a possible connection to Iran from the payment messages sent to the U.S.

65. More specifically, from 2002 to 2006, Intesa-Parma divided payment instructions, known as "SWIFT" messages,[8] involving Iranian bank treasury transactions or customer payments into two message streams.

66. The first SWIFT message included all details about the transaction, and Intesa-Parma would send it directly to the Iranian beneficiary's bank. Intesa-Parma would then send a second message, known as an MT202 or "cover payment" message, to Intesa-New York. The cover payment message did not include details about the underlying parties to the transaction and was sent in order to accomplish a transaction to be settled in U.S. dollars.

67. This process was designed to omit details included in the payment message sent to the New York Branch that might have been flagged by human or electronic scrutiny for possible OFAC violations, and which might have led the U.S. bank to delay or block the transaction. Nor would the Department be able to learn of the true nature of these transactions when carrying out its supervisory responsibilities.

68. Indeed, in a 2006 e-mail, an employee with the Head Office Compliance Department in Milan summarized the fundamental problem with Intesa's non-transparent

[8] The Society of Worldwide Interbank Financial Telecommunications ("SWIFT") provides an international network through which banks exchange electronic wire transfer messages. The SWIFT network offers various message types that can be used to transfer funds between banks; each type of message includes various informational fields.

processes: *"if we don't show the underlying links, we take away all possibility of controls by the authorities and/or the intermediary banks."*

69. Between approximately 2002 and 2006, the Bank conducted more than $11 billion of U.S. dollar transactions for Iranian entities through its non-transparent protocol. While such transactions may very well have been permissible under federal law and regulations at the time, New York and U.S. regulators were not able to thoroughly supervise the processing of these transactions because of the transactions' non-transparent nature.

70. Additionally, in conduct that occurred in the period October 2004 through March 2008, Intesa handled approximately $9 million of U.S. dollar transactions for Iranian, Sudanese and Cuban entities in apparent violation of federal sanctions laws and regulations. According to its settlement for $2.9 million with OFAC,

> Intesa had reason to know that one of its customers met the definition of the [Government of Iran under federal sanctions law], and that payments which terminated in the United States for this customer constituted apparent violations of [sanctions regulations]; Intesa's conduct resulted in harm to the integrity of U.S. economic sanctions programs; Intesa is a commercially sophisticated international financial institution; and Intesa did not at the time of the apparent violations, maintain an adequate program to ensure that it was in compliance with U.S. economic sanctions. Substantial mitigation was provided to Intesa due to the following factors: OFAC concluded that the apparent violations did not constitute a willful or reckless violation of the law; OFAC also determined that no Intesa managers or supervisors had actual knowledge or awareness of these matters within the meaning of the Guidelines; Intesa provided substantial cooperation to OFAC, including signing a tolling agreement and multiple extensions; Intesa took remedial action in response to the apparent violations and now has a more robust compliance program in place; and Intesa has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the transactions giving rise to the apparent violations.[9]

71. In early 2006, Intesa began revising its policies, and eventually blocked and then closed all of its Iranian U.S. dollar accounts between May and October 2007.

---

[9] *See* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20130628_intesa.pdf (penalty of approximately $3 million for conducting approximately 150 transactions).

Violations of Law and Regulations

72. Intesa Sanpaolo S.p.A. and Intesa Sanpaolo S.p.A. New York Branch failed to maintain an effective and compliant anti-money laundering program and OFAC compliance program, in violation of 3 NYCRR § 116.2.

73. Intesa failed to maintain and make available at its New York Branch true and accurate books, accounts, and records reflecting all transactions and actions, in violation of New York Banking Law § 200-c.

74. Intesa failed to submit a report to the Superintendent upon discovering omissions of true entries in violation of 3 NYCRR § 300.1.

75. Intesa failed to fully comply with the 2007 Written Agreement, which required Intesa to implement and maintain an effective BSA/AML compliance program.

Settlement Provisions

Monetary Payment

76. Intesa shall pay a civil monetary penalty pursuant to Banking Law § 44 to the Department in the amount of $235,000,000. Intesa shall pay the entire amount within ten days of executing this Consent Order. Intesa agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

Independent Consultant

77. Intesa shall extend the engagement of the Second Independent Consultant for the sole purpose of analyzing and testing the Bank's efforts to remediate the identified shortcomings in its BSA/AML compliance program and audit the Bank's transaction review efforts. All

findings and other results from this extended engagement of the Second Independent Consultant, including the reports, transaction review and audit described in Paragraphs 78-81, below, are intended for the sole purpose of informing the Bank's remediation efforts. Except as specified in Paragraphs 78-83, below, the Second Independent Consultant's work on the Expanded Look-Back shall be considered complete as of the execution of this Consent Order and payment of the civil monetary penalty by Intesa.

78. Within 60 days of full execution of this Consent Order, the Second Independent Consultant shall submit to the Department a report that summarizes its findings and conclusions concerning the Expanded Look Back (the "Look Back Report"). The Department shall make the Look Back Report available to Intesa for review and inspection.

79. Within 60 days of the full execution of this Consent Order, the Second Independent Consultant shall submit to the Department and the Bank a report that summarizes its findings, conclusions and recommendations concerning the effectiveness of Intesa-New York's compliance with applicable federal and state laws, rules and regulations relating to anti-money laundering policies and procedures, including but not limited to, under the BSA and Part 300 of the Superintendent's Regulations (the "Compliance Report").

80. The Second Independent Consultant shall prepare a written report assessing the implementation of the various remediation plans described in Paragraphs 84-88, below, within 60 days after receiving notice from the Bank that it has completed the remediation implementation.

81. The Bank will conduct a review of transactions processed by or through, or that otherwise pertain to or affect activities conducted by, the New York Branch, to identify and review missed alerts of the type described in Paragraph 44 and additional omissions or

deficiencies in transaction monitoring, if any, subsequently identified by the bank for the period 2014 to present, sufficient to reasonably ensure its compliance with all relevant laws, rules and regulations, including, but not limited to, the Bank Secrecy Act, federal sanctions laws, and New York laws, rules and regulations. The Independent Consultant shall perform a reasonable audit of those efforts and report on its audit to the Bank and the Department.

82. In connection with the Bank's obligations under Paragraph 81 above, Intesa shall take reasonable and necessary steps to ensure that all matters or transactions required by law to be reported, and that have not previously been reported, are duly reported in accordance with applicable laws, rules and regulations.

83. The extended term of the Independent Consultant shall be determined in the sole discretion of the Department in light of the remediation obligations set out in Paragraphs 77-88, but will not exceed two years. However, the Department retains the right to extend the term of the engagement if, in its sole discretion, it determines that an extension is necessary for the Bank to complete the remediation plans described in Paragraphs 84-88 below.

BSA/AML Compliance Program

84. Within sixty days (60) of the submission of the Compliance Report, Intesa-Milan and Intesa-New York shall jointly submit to the Department a written revised BSA/AML compliance program for Intesa-New York, acceptable to the Department. The program shall provide for:

a. a system of internal controls designed to ensure compliance with the BSA/AML Requirements and the state laws and regulations;

b. controls designed to ensure compliance with all requirements relating to correspondent accounts for foreign financial institutions;

c. a comprehensive BSA/AML risk assessment that identifies and considers all products and services of the New York Branch, customer types, geographic locations, and transaction volumes, as appropriate, in determining inherent and residual risks;

d. management of the New York Branch's BSA/AML compliance program by a qualified compliance officer, who is given full autonomy, independence, and responsibility for implementing and maintaining an effective BSA/AML compliance program that is commensurate with the New York Branch's size and risk profile, and is supported by adequate staffing levels and resources;

e. identification of management information systems used to achieve compliance with the BSA/AML requirements and the state laws and regulations and a timeline to review key systems to ensure they are configured to mitigate BSA/AML risks;

f. comprehensive and timely independent testing for Intesa-New York's compliance with applicable BSA/AML requirements and state laws and regulations; and

g. effective training for all appropriate Branch personnel and appropriate personnel of affiliates that perform BSA/AML compliance-related functions for Intesa-New York in all aspects of the BSA/AML requirements, state laws and regulations, and internal policies and procedures.

Suspicious Activity Monitoring and Reporting

85. Within sixty days (60) of the submission of the Compliance Report, Intesa-Milan and Intesa-New York shall jointly submit a written program to reasonably ensure the

identification and timely, accurate, and complete reporting by Intesa-New York of all known or suspected violations of law or suspicious transactions to law enforcement and supervisory authorities, as required by applicable suspicious activity reporting laws and regulations, acceptable to the Department. The program shall include:

a. a well-documented methodology for establishing monitoring rules and thresholds appropriate for the New York Branch's profile which considers factors such as type of customer, type of product or service, geographic location, and foreign correspondent banking activities, including U.S. dollar clearing activities;

b. policies and procedures for analyzing, testing, and documenting changes to monitoring rules and thresholds;

c. enhanced monitoring and investigation criteria and procedures to ensure the timely detection, investigation, and reporting of all known or suspected violations of law and suspicious transactions, including, but not limited to:

    i. effective monitoring of customer accounts and transactions, including but not limited to, transactions conducted through foreign correspondent accounts;

    ii. appropriate allocation of resources to manage alert and case inventory;

    iii. adequate escalation of information about potentially suspicious activity through appropriate levels of management;

    iv. maintenance of sufficient documentation with respect to the investigation and analysis of potentially suspicious activity, including the resolution and escalation of concerns; and

v. maintenance of accurate and comprehensive customer and transactional data and ensuring that it is utilized by Intesa-New York's compliance program.

Customer Due Diligence

86. Within sixty days (60) of the submission of the Compliance Report, Intesa-Milan and Intesa-New York shall jointly submit a written enhanced customer due diligence program, acceptable to the Department. The program shall include:

a. policies, procedures, and controls to ensure that Intesa-New York collects, analyzes, and retains complete and accurate customer information for all account holders, including, but not limited to, affiliates;

b. a plan to remediate deficient due diligence for existing customer accounts;

c. a revised methodology for assigning risk ratings to account holders that considers factors such as type of customer, type of products and services, geographic locations, and transaction volume;

d. for each customer whose transactions require enhanced due diligence procedures to:

i. determine the appropriate documentation necessary to verify the identity and business activities of the customer; and

ii. understand the normal and expected transactions of the customer;

e. policies, procedures, and controls to ensure that foreign correspondent accounts are accorded the appropriate due diligence and, where necessary, enhanced due diligence; and

f. periodic reviews and evaluations of customer and account information for the entire customer base to ensure that information is current, complete, and that the risk rating reflects the current information, and if applicable, documenting rationales for any revisions made to the customer risk rating.

Internal Audit

87. Within sixty days (60) of the submission of the Compliance Report, Intesa-Milan and Intesa-New York shall jointly submit a written revised internal audit program for Intesa-New York acceptable to the Department that shall provide for:

a. completion, at least annually, of a written Board of Directors-approved, risk-based audit plan that encompasses all appropriate areas of audit coverage;

b. timely escalation and resolution of audit findings and follow-up reviews to ensure completion of corrective measures; and

c. comprehensive tracking and reporting of the status and resolution of audit and examination findings to the Bank's Board of Directors.

Corporate Governance and Management Oversight

88. Within sixty days (60) of the submission of the Compliance Report, Intesa-Milan's board of directors and the management of Intesa-New York shall jointly submit to the Department a written plan to enhance oversight, by the management of Intesa-Milan and Intesa-New York, of Intesa-New York's compliance with BSA/AML requirements, state laws and regulations, and the regulations issued by OFAC acceptable to the Department. The plan shall provide for a sustainable governance framework that addresses, considers, and includes:

a. actions the board of directors will take to maintain effective control over, and oversight of, Intesa-New York's management's compliance with the BSA/AML requirements, state Laws and regulations, and OFAC regulations;

b. measures to improve the management information systems' reporting of Intesa-New York's compliance with BSA/AML requirements, state laws and regulations, and OFAC regulations to senior management of Intesa-Milan and Intesa-New York;

c. clearly defined roles, responsibilities, and accountability regarding compliance with BSA/AML requirements, state laws and regulations, and OFAC regulations for Intesa-Milan's and Intesa-New York's respective management, compliance personnel, and internal audit staff;

d. measures to ensure BSA/AML issues are appropriately tracked, escalated, and reviewed by Intesa-New York's senior management;

e. measures to ensure that the person or groups at Intesa charged with the responsibility of overseeing the Intesa-New York's compliance with BSA/AML requirements, state laws and regulations, and OFAC regulations possess appropriate subject matter expertise and are actively involved in carrying out such responsibilities;

f. adequate resources to ensure Intesa-New York's compliance with this Order, BSA/AML requirements, state laws and regulations, and OFAC regulations; and

g. a direct reporting line between the Head Office compliance officer and the board of directors or committee thereof.

Breach of Consent Order

89. In the event that the Department believes Intesa to be in material breach of the Consent Order, the Department will provide written notice to Intesa, and Intesa must, within ten business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

90. The parties understand and agree that Intesa's failure to make the required showing within the designated time period shall be presumptive evidence of the Bank's breach. Upon a finding that Intesa has breached this Consent Order, the Department has all the remedies available to it under New York Banking and Financial Services Law and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Waiver of Rights

91. The parties understand and agree that no provision of this Consent Order is subject to review in any court or tribunal outside the Department.

Parties Bound by the Consent Order

92. This Consent Order is binding on the Department and Intesa, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

93. No further action will be taken by the Department against Intesa for the conduct set forth in the Consent Order, provided that the Bank complies with the terms of this Consent Order.

Notices

94. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Megan Prendergast
One State Street
New York, NY 10004

James Caputo
One State Street
New York, NY 10004

Christine Tsai
One State Street
New York, NY 10004

For Intesa:

Piero Boccassino
Intesa Sanpaolo S.p.A.
Corso Inghilterra, 3
10138 Torino
Italy

Giuseppe La Sorda
Intesa Sanpaolo S.p.A.
Corso Inghilterra, 3
10138 Torino
Italy

Pierpaolo Monti
Intesa Sanpaolo S.p.A.
Corso Matteotti, 1
20121 Milano
Italy

Elisabetta Lunati
Intesa Sanpaolo S.p.A.
Via Verdi, 8
20121 Milano
Italy

Miscellaneous

95. Each provision of this Consent Order shall remain effective and enforceable until stayed, modified, suspended, or terminated by the Department.

96. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of the Consent Order.

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed this 15th day of December, 2016

INTESA SANPAOLO S.p.A.

By: _____
CARLO MESSINA
Managing Director & Chief Executive Officer of Intesa Sanpaolo S.p.A

INTESA SANPAOLO S.p.A.
NEW YORK BRANCH

By: _____
BIAGIO CALABRESE
Executive Vice President & General Manager of Intesa Sanpaolo S.p.A. New York Branch

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: _____
MARIA T. VULLO
Superintendent of Financial Services

By: _____
MATTHEW L. LEVINE
Executive Deputy Superintendent of Enforcement