SETTLEMENT AGREEMENT

This settlement agreement (the "Agreement") is made by and between Standard Chartered Bank and its subsidiaries and affiliates (collectively referred to hereafter as "SCB" or "Respondent") and the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC").

I. PARTIES

1. OFAC administers and enforces economic sanctions against targeted foreign countries, regimes, terrorists, international narcotics traffickers, and proliferation of weapons of mass destruction among others. OFAC acts under Presidential national emergency authorities, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction.

SCB is a financial institution registered and organized under the laws of England and Wales.

II. APPARENT VIOLATIONS

2. OFAC conducted an investigation of SCB in connection with thousands of transactions SCB processed to or through the United States in apparent violation of primarily the Iranian Transactions and Sanctions Regulations, 31 C.F .R. Part 560 ("ITSR"),[1] as well as a number of payments that implicated the now-repealed Sudanese Sanctions Regulations, 31 C.F.R. Part 538 ("SSR")[2], the Syrian Sanctions Regulations, 31 C.F.R. Part 542 ("SySR"), or Executive Order 13582 of August 17, 2011, "Blocking Property of the Government of Syria and Prohibiting Certain Transactions With Respect to Syria" (E.O. 13582), the now-repealed Burmese Sanctions Regulations, 31 C.F.R. Part 537 ("BSR"), and the Cuban Assets Control Regulations, 31 C.F.R. Part 515 (the "Apparent Violations").

3. OFAC determined that SCB did not voluntarily disclose the Apparent Violations, and that the Apparent Violations constitute an egregious case.

III. FACTUAL STATEMENT

4. On December 10, 2012, OFAC reached a $132,000,000 settlement with SCB regarding 911 transactions totaling approximately $133,076,791 it processed to or through the United States that appeared to have violated the ITSR, the now-repealed SSR, the now-repealed Libyan Sanctions Regulations, 31 C.F.R. Part 550, and the now-repealed BSR. OFAC determined that the apparent violations were egregious. OFAC's investigation determined that SCB, particularly the bank's London, UK operations ("SCB London") and Dubai, United Arab Emirates ("UAE") branches ("SCB Dubai"), engaged in payment practices that impaired compliance with U.S. economic sanctions by financial institutions in the United States, including SCB's branch office in New York, New York ("SCB NY"). Additionally, the 2012 settlement included eight apparent violations of the Foreign Narcotics Kingpin

[1] On October 22, 2012, OFAC changed the heading of 31 C.F.R. Part 560 from the Iranian Transactions Regulations to the ITSR, amended the renamed ITSR, and reissued them in their entirety. *See* 77 Fed. Reg. 64,664 (Oct. 22, 2012). For the sake of clarity, all references herein to the ITSR shall mean the regulations in 31 C.F.R. Part 560 at the time of the activity, regardless of whether such activity occurred before or after the regulations were reissued.

[2] As a result of the revocation of several sanctions provisions, effective October 12, 2017, U.S. persons may engage in transactions involving Sudan and the Government of Sudan without a general or specific OFAC license.

Sanctions Regulations ("FNKSR") by SCB NY, which occurred apart from the above conduct. Those apparent violations were determined to be non-egregious.

5. In the summer of 2013, OFAC became aware of specific information suggesting that the UAE-incorporated petrochemical company ("the petrochemical company")—which OFAC has concluded was (i) owned by an Iranian citizen and national; (ii) part of a network of companies that comprised an Iranian energy group; and (iii) engaged in the sale and transportation of petroleum products to, from, or through Iran—maintained a U.S. Dollar ("USD") relationship with SCB Dubai up to and including 2012.

6. Beginning in 2013 and over the next several years, at the request of OFAC and other federal and state government agencies and financial regulators, SCB engaged in a substantial investigation of SCB Dubai's relationship with the petrochemical company, as well as other corporate customers in SCB Dubai's Small and Medium Enterprise Banking ("SME") business that were tied to, or otherwise appeared to process transactions for, on behalf of, or involving, OFAC-sanctioned countries. This review included a number of "general trading companies" that appear to have facilitated USD transactions to or through SCB NY and/or other U.S. financial institutions by sending payment instructions to SCB Dubai via fax while physically located in Iran. The investigation expanded into the bank's internet and mobile banking platforms and identified a series of customers that accessed their accounts from Iran, Sudan, or Syria to initiate unauthorized commercial transactions to or through the United States.

The Petrochemical Company

7. OFAC's investigation of SCB revealed that SCB Dubai maintained an account for the petrochemical company, a company owned by an Iranian national ordinarily resident in Iran, which engaged in the sale of petroleum products to, from, or through Iran. Following OFAC's revocation of the U-Turn authorization on November 10, 2008, SCB, beginning no later than June 27, 2009, and, continuing through June 24, 2012, processed 190 transactions totaling $151,269,725 to or through the United States that were for or on behalf of the petrochemical company—the benefit of which services were received in Iran—in apparent violation of § 560.204 of the ITSR.

8. While it had previously blocked the account of its Iranian national beneficial owner (the "Iranian Person") due to sanctions risk, SCB Dubai maintained an account relationship for the petrochemical company even though it had information in its possession regarding the petrochemical company's Iranian ownership and business-related activities, and despite numerous warning signs over a period of several years regarding the company's Iranian connections, including direct communications with the petrochemical company, the receipt of emails and faxes from Iranian companies and/or telephone numbers, and the rejection of transactions involving the petrochemical company by U.S. financial institutions. SCB's failure to connect the information resulted in the bank continuing to process transactions involving the company for several years until blocking its account in December 2011 and finally closing the account in 2012.

9. On April 25, 2002, SCB Dubai opened a USD account for an individual in Iran (the Iranian Person). The account opening form for the Iranian Person identified his nationality as Iranian and listed a permanent address in Iran.

10. Several years later, on May 17, 2005, after a meeting between an SCB Dubai Relationship Manager ("RM") and the Iranian Person (who was the petrochemical company's sole shareholder), SCB Dubai opened a UAE Dirham and USD-denominated account for the petrochemical company. The Certificate of Formation and Share Certificate provided to SCB's representative office in Tehran, Iran ("SCB Tehran") in connection with later discussions that were unrelated to the account opening listed the registered owner of the petrochemical company as the Iranian Person and recorded his address as a near identical match to the address on file for the Iranian Person's personal USD account with SCB Dubai. SCB Dubai received an Iranian passport and UAE residence visa for the Iranian Person, as well as documents showing that the petrochemical company was located and operated in the Dubai Airport Free Zone.

11. In addition to the above-referenced connections between the Iranian Person and the petrochemical company, personnel at SCB Dubai and SCB Tehran received emails, trade proposals, and other documentation over the course of the next several years demonstrating the petrochemical company's ties to, and business activities with, Iran. An organizational chart in SCB Tehran's possession that was obtained in July 2006 by an SCB Dubai sales employee listed the petrochemical company as part of a group of seven companies—three of which were incorporated and located in Iran. The organizational chart, which the bank asserts that the SCB Dubai sales employee did not share with anyone else at SCB Dubai, included background information on the petrochemical company group. It identified the Iranian Person as "the owner of the total company shares and General Manager," and described several of its business activities as related to the sale, purchase, and transportation of liquefied petroleum gas and other petroleum products from, to, or through Iran. In addition, on at least one occasion, SCB Dubai received an email from the Financial Manager of the petrochemical company's Tehran Branch that included an identical fax number to the fax number provided in the aforementioned organizational chart for a named Iranian-incorporated company.

12. In 2005, SCB Dubai began implementing an Iran-related tagging procedure across its customer database as part of the bank's efforts to identify accounts held by UAE customers with ties to Iran. In late September 2005, SCB Dubai's then-Group Legal Counsel authored the "Iran Supplement," which summarized the bank's understanding of U.S. sanctions against Iran and their impact on SCB's non-U.S. offices. The bank ultimately determined that it could create a "tag" or "refer marker" called "IRA" that would be applied to accounts held by SCB Dubai customers with ties to Iran. During this process, SCB Dubai identified the personal account of the Iranian Person because the bank's core banking system (known as eBBS) identified the Iranian Person as Iranian in one or more of the nationality, domicile, or residency fields. These searches did not identify the petrochemical company's account, however, despite the numerous connections that existed between the Iranian Person and the petrochemical company.

13. In and around the summer of 2007, SCB Dubai maintained a series of compliance controls designed to prevent the bank from processing transactions in violation of U.S. sanctions. However, the controls were often insufficient for OFAC purposes, and in some cases were not closely followed by SCB Dubai staff. For example, SCB Dubai relied heavily on the information it collected for each of the bank's customers in Customer Due Diligence (CDD) files. SCB Dubai RMs for corporate accounts (including the petrochemical company) were required to collect standard information regarding the bank's customers, including contact details, and add the information to the customer's CDD File. In October 2007, the CDD for the Iranian Person's individual account identified the Iranian Person as "resident in a [high risk jurisdiction] —Iran" and also noted that the Iranian

Person remitted/received money directly to or from a sanctioned country. The CDD documents for the petrochemical company, which identified "the sole owner of [the petrochemical company]" as the Iranian Person, were marked "YES" to the following questions:

- Is the client a sanctioned country government (anywhere in the world)?
- Is the client a sanctioned country government-owned bank or other enterprise (anywhere in the world), including subsidiaries, branches and offices thereof?
- Is the client a company incorporated in, or an unincorporated firm based in . . . a Sanctioned Country . . . ?
- Does the client trade in products or services that originate in a Sanctioned Country or import goods or services of any origin from a Sanctioned Country?
- Does the client export any goods or services either directly to a Sanctioned Country or to a Sanctioned Country via another country?
- Does the client remit/receive any money directly to/from a Sanctioned Country or indirectly via another country?

14. Despite the connections between the Iranian Person's personal account and the petrochemical company account, as well as the indications and CDD forms that explicitly identified the company's Iranian-related business activities, SCB did not identify the two accounts as linked within its internal systems.

15. In early-to-mid 2008, the SCB Dubai RM for the petrochemical company ("the petrochemical company's RM") received two direct communications from the Iranian Person requesting that the petrochemical company's contact information be updated within the bank's systems. Both communications were faxes that originated from Iran. Specifically, on April 10, 2008, the Iranian Person sent a fax to the petrochemical company's RM in order to update the contact information on file at the bank for the company. The fax also included contact numbers for a "Tehran Representative Office" of the petrochemical company. The fax number provided in the communication to SCB Dubai was identical to the fax number listed in the aforementioned organizational chart for one of the Iranian-incorporated companies in the petrochemical company group, and also listed an email address which contained the name of the Iranian Person and the petrochemical company group.

16. Despite the above-referenced communications, in 2009 SCB Dubai updated the petrochemical company's CDD file and changed most of the sanctions-related questions (which, as noted above, had been marked as "YES" in October 2007) to "NO"—including whether the company was incorporated in, a branch or agent of a company incorporated in, or majority-owned by an individual resident of a sanctioned country. Although the payment messages that SCB Dubai processed to or through the United States involving the petrochemical company identified the company by its name, they did not include references to Iran, the petrochemical company's Iranian ownership, or any affiliated Iranian entities. Most of the transactions originated by SCB Dubai on behalf of the petrochemical company were processed successfully and reached their intended beneficiary.

17. On several occasions, U.S. financial institutions acting as intermediaries obtained information that led them to reject payments involving the petrochemical company pursuant to the ITSR. For example, on February 8, 2010, SCB Dubai originated a $100,000 funds transfer on behalf of the petrochemical company, through SCB NY and another U.S. financial institution located in New

York (the "U.S. Bank"), destined for a third-country company's account at the central bank of a third country. Upon receipt of the payment instructions, the U.S. Bank stopped and rejected the transaction, citing that the purpose of the payment as involving an Iranian financial benefit.

18. On April 26, 2010, a senior director within the Financial Crimes Risk (FCR) unit of SCB Americas ("Senior FCR Director in New York") sent an email to the senior anti-money laundering officer ("Senior AML Officer in Dubai"), and operational risk manager for SME at SCB Dubai ("Operational Risk Manager in Dubai"), and the manager of Gulf credit operations ("Credit Operations Manager") informing them that the aforementioned U.S. Bank had rejected an additional April 19, 2010 funds transfer with a value of $40,000 originated by SCB Dubai on behalf of the petrochemical company. The Senior FCR Director in New York stated: "In the [Originator to Beneficiary Information] field of the return payment [the U.S. Bank] stated: 'REJECT for [the petrochemical company] per OFAC.'" The email continued and noted "[SCB NY] contacted the [U.S. Bank] and they advised their research shows [the petrochemical company] as located in Iran."

19. On April 27, 2010, several SCB Dubai personnel engaged in an internal discussion regarding the petrochemical company in response to the Senior FCR Director in New York's above-referenced email. In an email addressed to the Operational Risk Manager in Dubai and copying the petrochemical company RM and the senior manager for portfolio management and distribution for SME ("Senior SME Portfolio Manager"), an SCB Dubai employee provided some background information on the petrochemical company's account, and made the following statements: "There is only one owner in the company whose name is [the Iranian Person] [and the] owner is an Iranian national."

20. Subsequently, the Operational Risk Manager in Dubai emailed the Senior SME Portfolio Manager and noted the following:

> I found [in SCB Dubai's internal document management system] a notice from [the petrochemical company] dated 10th April 2008 to the attention of [the petrochemical company's RM], requesting for the update of [the petrochemical company's] contact nos. in Dubai including that of their representative office in Tehran. And, those contact details were updated in the system. When I checked the company's name from google I found the same . . . with nationality as "Iran" and the email ID per our record matches with that found in google. Also, the UAE visa of the owner, [the Iranian Person] expired in 2008.

21. Later the same day, the Operational Risk Manager in Dubai emailed the Senior AML Officer in Dubai and stated that he/she "strongly believe[s] that the subject customer [the petrochemical company] is an Iranian." The Senior AML Officer in Dubai replied that the matter would be escalated to a senior sanctions officer in the U.K. ("Senior Sanctions Officer in the U.K.") and that the Senior AML Officer in Dubai would determine what information should be sent to SCB NY.

22. Following a May 6, 2010 meeting with the Iranian Person, the petrochemical company RM sent an email directly to SCB NY and stated that the petrochemical company's physical address was located in Dubai. The petrochemical company RM further noted that the Iranian Person had stated the petrochemical company had "nothing to do with" Iran, but explained that he relied solely on the

Iranian Person's representations and did not receive any documentation to support these claims. The response noted that the Iranian Person's "nationality is Iranian but holds a valid UAE residence visa and carries out [the petrochemical company's] [o]perations from Dubai." Although the petrochemical company's CDD file contained a residence visa for the Iranian Person valid from 2008-2011 and 2011-2014, the response did not note that the Iranian Person's UAE residence visa expired in 2008 (which was raised by the Operational Risk Manager in Dubai and had been retrieved from SCB Dubai's internal document management system), nor does it appear that SCB Dubai performed a further review of the petrochemical company's ownership or business activities prior to sending this information to SCB NY.

23. SCB NY replied to the petrochemical company RM's email and questioned whether "[the petrochemical company] in the link below is not affiliated with [the petrochemical company]," and provided an internet hyperlink to an Iranian entity with the same name (and presumably the same information raised by the Operational Risk Manager in their email to the Senior SME Portfolio Manager). The petrochemical company's RM indicated that, based on an interview with the customer, the customer represented that the petrochemical company "has no operation or any other links with Iran." The petrochemical company's RM also noted that the petrochemical company's contact information on file with SCB Dubai did not match the contact information in the hyperlink. The Senior FCR Director in New York subsequently forwarded this email to the Senior Sanctions Officer in the U.K.

24. On May 20, 2010, SCB NY sent a letter to OFAC regarding the April 19, 2010 rejected transaction. In its one-page letter to OFAC, SCB NY stated that it contacted SCB Dubai to obtain confirmation regarding the originator:

> [SCB Dubai] advised us that the originator, [the petrochemical company], is located not in Iran but [in the] Dubai Airport Free Zone, Dubai, UAE. It is 100% owned by [the Iranian Person]. His nationality is Iranian but he holds a valid UAE residence visa and carries out the company's operations from Dubai. The account is used in connection with liquid petroleum gas purchases . . . from Turkmenistan and sales to Armenia, Pakistan and Iraq. The customer confirmed that this payment was made under such a transaction and there was no direct or indirect involvement with Iran. We therefore believe the payment was permitted.

25. Despite the numerous payments rejected by other U.S. financial institutions involving the petrochemical company, as well as the concerns raised internally within SCB Dubai regarding the petrochemical company's Iranian ownership and connections, both SCB Dubai and SCB NY continued to process USD payments on the company's behalf. In total, SCB Dubai and SCB NY processed 133 funds transfers totaling $140,310,539 that were for or on behalf of the petrochemical company to or through the United States in apparent violation of the ITSR *after* May 2010 (the date on which senior-level personnel within SCB Dubai and SCB NY discussed the petrochemical company's Iranian-related connection following the U.S. Bank's rejection of the April 2010 transaction).

26. On September 20, 2011, SCB Dubai decided to exit its account relationships with the petrochemical company due to concerns about the entity's relationship with Iran. A series of internal emails among SCB Dubai's Compliance staff, including the Senior AML Officer in Dubai, demonstrated that the bank had determined that "one of the partner [sic] has another company . . .

whose web site is confirming that they do business with Iran." The CDD checklist for the petrochemical company also identified the company's risk level as enhanced due diligence due to concerns about Iranian nationals as shareholders. The CDD addendum associated with these files also indicated that the Iranian Person had not provided additional proof of residency outside of Iran.

27. In March 2012, an origination and client coverage accountable representative ("OCC Representative") met with the Iranian Person and subsequently sent his meeting recollections to a senior regional financial crime risk officer in the UAE ("Senior Regional FCR Officer in the UAE"). In the course of the meeting, the OCC Representative noted that the Iranian Person was unable to provide documentation showing that the petrochemical company was separate from the petrochemical company group, or that it had bona fide operations outside of Iran. In addition, the Iranian Person "admitted that while [the petrochemical company's] business may on paper not be related to Iran, the fact that he also owns [the petrochemical company group] whose business is almost solely in/with the [oil and gas] sector in Iran effectively prevents the bank from doing business with him."

28. In December 2011, SCB Dubai blocked all transactional activity in, and commenced the process of closing, the petrochemical company's accounts. In June 2012, SCB Dubai added the names of the petrochemical company and the Iranian Person to its transaction filters, and closed all of the petrochemical company's accounts with the bank.

Faxed Payment Instructions Received by SCB Dubai from Iran

29. During the course of OFAC's investigation of SCB in relation to the petrochemical company, the bank produced documents suggesting that the petrochemical company faxed USD-denominated payment instructions to SCB Dubai from Iran. These payment instructions were used by SCB Dubai to originate a number of outgoing transactions for or on behalf of the petrochemical company that the bank processed to or through the United States. SCB subsequently devised a methodology to search its available records for, and undertook a comprehensive review of, payment instructions faxed to its branch offices in the UAE from Iran based on fax numbers beginning with a country code of +98, 98, or 0098 and identified 11,809 faxed payment instructions from 176 distinct SCB Dubai customers, all of which were corporate or commercial entities. That review determined that faxes from Iran ceased in September 2012 due to other compliance measures even though the Bank did not block such fax access in the UAE until May 2014.

30. SCB Dubai officials appear to have had actual knowledge that some of the bank's customers were misusing or misrepresenting their UAE residency and, instead, were ordinarily resident in or conducting business with or from Iran. Although SCB Dubai was in possession of information and other data points connecting several of its customers to Iran or Iranian-related payments, and received numerous warning signs from various SCB personnel and other financial institutions that rejected transactions involving SCB Dubai customers, the bank failed to implement proper controls or conduct a reasonable level of due diligence to identify problematic customers and prohibited transactions.

31. Two SCB Dubai corporate customers, General Trading Company A ("Company A") and General Trading Company B ("Company B"), both of which were minority-owned by the same Iranian individual, generated the majority of the transaction volume in this category of apparent violations by issuing faxed payment instructions from Iran. UAE law requires that companies

incorporated outside of a free zone must be majority owned by a UAE national. The bank failed to respond to numerous warning signs regarding the suspicious activities of these parties or failed to conduct an appropriate review of their business activities and transaction volume. In several instances two employees within SCB Dubai—including a Relationship Manager associated with several general trading company accounts—actively worked with the account holders to obfuscate the sanctions nexus associated with the parties and/or their transactions, misled or made false statements to other SCB personnel regarding these companies, and attempted to assist the parties in concealing their identity and/or opening new accounts once SCB Dubai had terminated the customer relationship.

32. On December 21, 2006, an Iranian national ("Iranian Person #2") opened an account at SCB Dubai for Company A. SCB Dubai obtained or prepared various forms of documentation during the account opening stage, including: a scanned copy of Iranian Person #2's Iranian passport; a copy of the Government of Dubai's commercial license issued to Company A, which identified the nationality of the company's manager (presumably Iranian Person #2) as Iranian; and account opening documentation. Beginning no later than December 2007, the Company A account generated a number of internal alerts within SCB Dubai regarding the company's transaction activity. For example, between December 26, 2007 and October 19, 2008, SCB Dubai made six separate internal unusual activity referrals to its anti-money laundering unit regarding Company A. Separately, between April 18, 2008 and January 25, 2011, approximately 33 Company A-initiated transactions were escalated within SCB Dubai for review.

33. In some cases, the referrals and escalations specifically noted that Company A may have a nexus to or conduct business with Iran. Several U.S. banks rejected or returned payments initiated from Company A's account with SCB Dubai as early as July 2008. With respect to two such transactions, the financial institutions that submitted reports to OFAC stated that they suspected (though were not able to confirm) that the beneficiaries were located in Iran.

34. In August 2010, a U.S. bank rejected a payment initiated by Company A from its account with SCB Dubai. In subsequent correspondence to OFAC, SCB NY stated:

> We contacted SCB Dubai to obtain further information. [Company A] has been a client since 2006 and has an address [in] Dubai, UAE. [A named UAE Individual] owns 51% and is a resident of Dubai and [Iranian Person #2] owns 49% and is an Iranian national based in UAE with a valid residential visa. SCB Dubai advised their customer is a general trader in many products including power tools and circuits for printing, diamond, and car industries mainly for China, Middle East, and Europe.

35. Internal emails show that the U.S. bank that rejected the payment provided SCB NY with information stating that the "true originator is . . . located in Tehran, Iran." Several months later, in October 2010, Company A submitted updated contact information to SCB Dubai that provided two mobile numbers and an office fax number in Iran.

36. In December 2010, the senior cash management employee for Europe ("Senior Cash Management Employee") emailed senior managers from SCB Dubai regarding a large number of rejected payments from European correspondents that were destined for or otherwise involved account holders at SCB Dubai. The email listed several companies, including Company A, for which SCB

Germany would now decline all payments due to concerns regarding the Iran sanctions. The Senior Cash Management Employee noted:

> We are receiving messages from the below customers and have effected [the payments]. However, they have then been returned by the EURO correspondent banks saying that the entities have Iranian connections. Our compliance has instructed us to place these names in our filter in MTS (FFT payment system) and to reject . . . . My question is that if these were Iranian entities I would have thought you would have closed the accounts in Dubai's books. Obviously, banks have the right to refuse payments we send (we do the same to payments we receive) but I am a little concerned that our Compliance area have told us to do this without a Group wide directive coming from the [GSA]. I just wondered if you could comment/if you were aware that we were refusing your payments from these customers.

37. On January 2, 2011, the Operational Risk Manager in Dubai emailed several bank personnel—including Company A's RM—and noted: "I copied the screenshot from eBBS which shows that [Iranian Person #2] is an Iranian person, being a non-resident. In the contact details, I found contact numbers in Iran. Can you please ascertain this information, if this is the case we need to act on this immediately by referring the case to FCR." Two weeks later, Company A's RM responded and confirmed: "The owner [Iranian Person #2] is an Iranian national and has residence in Dubai and has frequent travels between Dubai-Turkey-Iran.... This account is also in process of closure as we have a strong suspicion for Iran related transactions evident from the transactions being stuck in Filtering que [*sic*]."

38. A few days later, Company A's RM and Iranian Person #2 had a phone call regarding the status of the Company A's account closure. In a translated and transcribed copy of the conversation, the RM agreed to try to postpone the closure of Company A's account for a few weeks and also discussed another one of Iranian Person #2's companies named Company B.

39. SCB Dubai opened an account for Company B on August 25, 2010, but closed it on February 7, 2011 without ever having processed a transaction. Several days after closing the first account for Company B, and one day after SCB officially closed Company A's account, SCB Dubai opened a second account for Company B on February 14, 2011. While the company identified one of the shareholders as a certain unnamed individual, several documents connected Company B to Company A.

40. For example, Company B's email contact information was the same as one of the email addresses utilized by Company A. The account-opening documentation prepared by SCB Dubai also listed Company A as one of Company B's significant buyers or suppliers. In addition, in an official company mandate dated February 23, 2011, Company B stated: "the persons named in the Schedule to the Letter [are hereby] authorized to act on behalf of the Company in the manner specified therein." The schedule to the letter listed Iranian Person #2 as an authorized dealer and signatory for Company B's account (including the ability to enter into any financial transactions).

41. Almost immediately following the opening of the second Company B account, SCB Dubai escalated numerous payments involving the company for review (a total of 15 between March 2011 and July 2011). On March 3, 2011, the SCB Sanctions Filtering unit stopped an outgoing non-

USD funds transfer originated by Company B from its account with SCB Dubai that was destined for a third-country bank's customer. SCB Dubai cancelled the payment after confirming the underlying purpose of the payment was related to Iran. In or around this time, the RM held several phone calls with Iranian Person #2 regarding these transactions. The RM appears to have referenced prior discussions in which he had coached Iranian Person #2 how to process certain types of transactions.

42. In a series of internal emails among SCB Dubai personnel, the RM stated that he spoke with the account owner of Company B (the unnamed Person) who denied any relationship with Company A. On July 7, 2011, SCB Dubai sent Company B a letter stating that the bank would be closing its USD account. SCB Dubai eventually closed the account on September 4, 2011. In addition, the client failed to respond to multiple SCB inquiries requesting additional details regarding the company's use of the account. Throughout the duration of Company B's account relationship with the bank (specifically the second account), SCB Dubai processed 210 USD-denominated funds transfers to or through the United States based on payment instructions it received from Iran.

43. OFAC determined that the transactions SCB processed to or through the United States, which involved Company A, Company B, or other corporate entities that initiated payment instructions from Iran, constitute apparent violations of § 560.204 of the ITSR.

Online Payments from Countries Subject to Comprehensive Sanctions

44. During the course of the same investigation, the bank reviewed its online and mobile banking platforms. The bank's review revealed that SCB did not take appropriate measures to ensure that online banking transactions initiated from countries subject to comprehensive OFAC-administered sanctions were compliant with applicable prohibitions until 2014, despite multiple supervisory and management personnel in various business lines having actual knowledge of, and having discussions pertaining to, the sanctions risks associated with these specific products and services. SCB's failure to implement controls and measures to address this issue in a timely manner caused the bank to process thousands of transactions through SCB NY on behalf of corporate customers located in, or that related to commercial activity involving, countries subject to comprehensive U.S. economic sanctions.

45. SCB appears to have received numerous warning signs, and subsequently engaged in substantial internal discussions, regarding certain risks and potential violations associated with customers accessing their accounts through the internet from sanctioned jurisdictions by no later than 2011. However, SCB failed to fully appreciate the scope and magnitude of this issue within the bank—including the number of SCB systems implicated.

46. By no later than March 2012, various SCB compliance, legal, and business personnel, including those in supervisory and/or managerial positions, engaged in a lengthy internal discussion regarding customers accessing their accounts from countries subject to comprehensive U.S. economic sanctions.

47. In a March 22, 2012 email, the Senior Regional FCR Officer in the UAE expressed concerns that customers were logging in from Iran to initiate payments and raised the issue with the Senior Sanctions Officer in the U.K. and a senior sanctions officer in the U.S. ("Senior Sanctions Officer in the U.S."), and copied several other individuals on the email. A day before, the senior IT

employee for Wholesale Banking ("Senior IT Employee") had emailed the Senior Regional FCR Officer in the UAE, stating:

> If the business agrees, IP addresses from Iran can be blocked HOWEVER due to the changing nature of IP addresses we cannot guarantee all IP addresses are blocked and that we are not blocking legitimate clients . . . . Previous discussions with Business in regards to blocking blacklisted IP addresses have resulted in reporting only. Rather than block, I suggest reporting on addresses believed to be from Iran—on the assumption there is someone available to take action.

48. On April 30, 2012, the Senior Sanctions Officer in the U.S. sent an email to an IT employee, the Director, Transaction Banking Payment and the Deputy Head of Financial Crimes Compliance copying the Senior Sanctions Officer in the U.K., regarding these issues:

> In summary, SCB Dubai recently discovered (as part of a non-sanctions related review of data from S2B) that it appeared that a number of clients had accessed S2B through Iranian Internet Service Providers, suggesting that the clients were in Iran when they did so. SCB Dubai is following up with those clients to see what explanation they can offer, but it does raise a wider question of how we can monitor/prevent such access, as payments instructed by parties in Iran (or other sanctioned countries) could cause sanctions issues. While S2B is the channel that this incident has involved, there must also be a wider question relating to other electronic banking channels.

49. Internal emails show that SCB did not leverage data from accounts accessing SCB platforms in Iran to conduct relationship reviews.

50. Several weeks later, on June 8, 2012, the Senior Sanctions Officer for the U.K. sent an email to the Senior Sanctions Officer in the U.S. and other personnel regarding the above-referenced sanctions-related issues with SCB's online banking systems and concluded the following: "The S2B system has the capability to block access to all clients, by country from which access is sought . . . . The blocking process would take 2-3 weeks after internal approvals are obtained."

51. By September 2012, SCB had not limited or restricted access to its online banking platforms from comprehensively sanctioned jurisdictions, but concluded that over 3,500 discreet log-ins had occurred in comprehensively sanctioned countries throughout 2012.

52. Personnel within SCB maintained that the bank should not block access to its online banking platform because there were certain technical limitations which might not prevent all log-ins from jurisdictions subject to comprehensive sanctions, and the blocking could negatively impact the customer experience.

53. Although SCB did not move to successfully block access to online banking from jurisdictions subject to comprehensive sanctions at the time, the bank had the capability to block access from IP addresses associated with certain countries and, in at least one earlier instance in 2010, did so for a non-sanctions-related issue.

54. SCB did not implement any controls to restrict access from jurisdictions subject to comprehensive sanctions until April 2013, when it blocked S2B access from sanctioned countries and July 2014 when the bank similarly blocked access to the i-banking system.

As a result of the activities described above:

55. Between June 2009 and May 2014, SCB processed 7,710 transactions totaling $333,967,499 to or through financial institutions in the United States pursuant to several Iran-related credit facilities, 689 fax payments with a value of $35,348,468, and 705 USD-denominated online payments to or through the United States with a total value of $46,911,754 in apparent violation of § 560.204 of the ITSR, which prohibits the direct or indirect exportation of services to Iran from the United States or by a U.S. person.

56. Between July 2010 and May 2014, SCB processed approximately three fax payments with a total value of $212,480 to or through financial institutions in the United States, and 131 USD-denominated online payments to or through the United States with a total value of $7,581,311 in apparent violation of § 538.205 of the SSR, which prohibited the exportation or reexportation, directly or indirectly, to Sudan of any services from the United States or by a U.S. person.

57. Between August 2011 and June 2014, SCB processed approximately 63 fax payments totaling $9,732,971 to or through financial institutions in the United States, and 16 USD-denominated online payments to or through the United States with a total value of $86,446 in apparent violation of E.O. 13582 or § 542.207 of the SySR, which prohibits the exportation or reexportation, directly or indirectly, to Syria of any services from the United States or by a U.S. person.

58. Between July 2012 and April 2013, SCB processed approximately 17 USD-denominated online payments to or through the United States with a total value of $3,709,451 in apparent violation of § 515.201 of the CACR, which prohibits, *inter alia*, dealings by persons subject to the jurisdiction of the United States involving property in which a national of Cuba has any interest of any nature whatsoever, direct or indirect.

59. Between May 2009 and May 2012, SCB processed approximately one USD-denominated online payment to or through the United States with a total value of $3,000 in apparent violation of § 537.202 of the BSR, which prohibited the exportation or reexportation, directly or indirectly of financial services to Burma from the United States or by a U.S. person.

60. Since 2013, SCB has undertaken a comprehensive global remediation of its sanctions compliance program. As part of its remediation, SCB has taken a number of steps, including: forming a special board committee with responsibility for overseeing SCB's overall financial crime compliance program; implementing additional and more rigorous U.S. sanctions policies and procedures; spending $2.8 billion on financial crime compliance since 2012; hiring new senior leadership and increasing its staff in its legal and financial crime compliance functions six-fold since 2012; certifying that it has trained relevant employees on complying with U.S. economic sanctions laws and regulations; implementing additional measures to block payment instructions from countries subject to U.S. sanctions laws and regulations; providing compliance training programs for SCB's global correspondent banking clients; upgrading its customer due diligence, transaction screening, and other

compliance tools and technology; and improving its ability to assess and measure its sanctions compliance risk, to ensure its U.S. economic sanctions compliance program is effective.

61. Beyond its internal remediation efforts, SCB has worked proactively to devise, implement, and support new models of industry cooperation to detect and prevent financial crime, including through public-private partnerships.

62. SCB fully cooperated with OFAC's investigation, including (1) through the production of a voluminous quantity of documents, (2) through presentations of the bank's own extensive and thorough internal investigation laying out the facts, bringing the misconduct of two former junior employees to OFAC's attention, and answering numerous follow-up inquires for information over the course of OFAC's investigation, and (3) by entering into a statute of limitations tolling agreement and multiple extensions to the agreement.

IV. TERMS OF SETTLEMENT

OFAC and Respondent agree as follows:

63. In consideration of the undertakings of Respondent in paragraph 64 below, OFAC agrees to release and forever discharge Respondent, without any finding of fault, from any and all civil liability in connection with the Apparent Violations, as described in paragraphs 55-59, or any activities that were the subject of OFAC's investigation, arising under the legal authorities that OFAC administers.

64. In consideration of the undertakings of OFAC in paragraph 63 above, Respondent agrees to a settlement in the amount of **$639,023,750.** Respondent's obligation to pay OFAC such settlement amount shall be deemed satisfied up to an equal amount by payments in satisfaction of penalties assessed by U.S. federal agencies arising out of the same patterns of conduct during the same time periods. Respondent further agrees and represents:

A. Within fifteen (15) days of the date Respondent receives the unsigned copy of this Agreement, to sign, date, and mail an original signed copy of this Agreement to the Office of Foreign Assets Control, U.S. Department of the Treasury, Attn: [redacted], Sanctions Compliance and Evaluation Division, 1500 Pennsylvania Avenue, NW, Washington, DC 20220. Respondent should retain a copy of the signed Agreement and a receipt or other evidence that shows the date that Respondent mailed the signed Agreement to OFAC;

B. To waive (i) any claim by or on behalf of Respondent, whether asserted or unasserted, against OFAC, the U.S. Department of the Treasury, and/or its officials and employees arising out of the facts giving rise to the enforcement matter that resulted in this Agreement, including but not limited to OFAC's investigation of the Apparent Violations, and (ii) any possible legal objection to this Agreement at any future date.

C. **Compliance Commitments:** Respondent has terminated the conduct described in paragraphs 4-54 and has undertaken comprehensive global remediation of its sanctions compliance program. As a result, Respondent has established, and agrees to maintain, sanctions compliance measures that are designed to minimize the risk of recurrence of

similar conduct in the future. Specifically, OFAC and Respondent understand that the following compliance commitments have been made:

a. **Management Commitment:**

i. Respondent commits that Senior Management has reviewed and approved Respondent's sanctions compliance program.

ii. Respondent commits to ensuring that its senior management, including senior leadership, executives, and/or the board of directors, are committed to supporting Respondent's sanctions compliance program.

iii. Respondent commits to ensuring that its compliance unit(s) are delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls Respondent's OFAC risk.

iv. Respondent commits to ensuring that its compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to Respondent's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

v. Respondent commits to ensuring that Senior Management promotes a "culture of compliance" throughout the organization.

vi. Respondent's Senior Management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, and acknowledges its understanding of the apparent violations at issue, and commits to implementing necessary measures to reduce the risk of reoccurrence of similar conduct and apparent violations from occurring in the future.

b. **Risk Assessment:**

i. Respondent conducts an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. The risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by Respondent during the routine course of business.

ii. Respondent has developed a methodology to identify, analyze, and address the particular risks it identifies. The risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by Respondent during the routine course of business, for example, through a testing or audit function.

c. **Internal Controls:**

i. Respondent has designed and implemented written policies and procedures outlining its sanctions compliance program. These policies and procedures are relevant to the organization, capture Respondent's day-to-day operations and procedures, are easy to follow, and prevent employees from engaging in misconduct.

ii. Respondent has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable Respondent to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into Respondent's internal controls, Respondent has selected and calibrated the solutions in a manner that is appropriate to address Respondent's risk profile and compliance needs, and Respondent routinely tests the solutions to ensure effectiveness.

iii. Respondent commits to enforcing the policies and procedures it implements as part of its sanctions compliance internal controls through internal and/or external audits.

iv. Respondent commits to ensuring that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.

v. Respondent commits to ensuring that, upon learning of a weakness in its internal controls pertaining to sanctions compliance, it will take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

vi. Respondent has clearly communicated the sanctions compliance program's policies and procedures to all relevant staff, including personnel within the sanctions compliance function, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing sanctions compliance responsibilities on behalf of Respondent.

vii. Respondent has appointed personnel to integrate the sanctions compliance program's policies and procedures into Respondent's daily operations. This process includes consultations with relevant business units, and ensures that Respondent's employees understand the policies and procedures.

d. **Testing and Audit:**

i. Respondent commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, and resources within the organization.

ii. Respondent commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its sanctions compliance program and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of Respondent's OFAC-related risks and internal controls.

iii. Respondent commits to ensuring that, upon learning of a confirmed negative testing or audit result pertaining to its sanctions compliance program, it will take immediate and effective action to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.

e. **Training:**

i. Respondent commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support Respondent's sanctions compliance efforts.

ii. Respondent commits to providing OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.

iii. Respondent commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile and, at a minimum, at least once a year to all relevant employees.

iv. Respondent commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its sanctions compliance program, it will take immediate and effective action to provide training to relevant personnel.

v. Respondent's training program includes easily accessible resources and materials that are available to all applicable personnel.

f. **Annual Certification:**

On an annual basis, for a period of five years, starting from 180 days after the date the Agreement is executed, a senior-level executive or manager of Respondent will submit to OFAC a certification confirming that Respondent has implemented and continued to maintain the sanctions compliance measures as committed above.

65. Should OFAC determine, in the reasonable exercise of its discretion, that Respondent appears to have materially breached its obligations or made any material misrepresentations under subparagraph C of paragraph 64 (Compliance Commitments) above, OFAC shall provide written notice to Respondent of the alleged breach or misrepresentations and provide Respondent with 30 days from the date of Respondent's receipt of such notice, or longer as determined by OFAC, to determine that no material breach or misrepresentations has occurred or that any breach or misrepresentation has been cured.

66. In the event OFAC determines that a material breach of, or misrepresentation in, this Agreement has occurred due to a failure to perform the Compliance Commitments, OFAC will provide notice to Respondent of its determination and whether OFAC is re-opening its investigation. The statute of limitations applying to the Apparent Violations shall be deemed tolled until a date 180 days following Respondent's receipt of notice of OFAC's determination that a breach of, or misrepresentation in, this Agreement has occurred.

67. Should the Respondent engage in any other violations of the sanctions laws and regulations administered by OFAC—including those that are either apparent or alleged—OFAC may consider Respondent's sanctions history, or its failure to employ an adequate sanctions compliance program or appropriate remedial measures, associated with this Agreement as a potential aggravating factor consistent with the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, Appendix A.

68. This Agreement does not constitute a final agency determination that a violation has occurred, and shall not in any way be construed as an admission by Respondent that Respondent engaged in the Apparent Violations.

69. This Agreement has no bearing on any past, present, or future OFAC actions, including the imposition of civil monetary penalties, with respect to any activities by Respondent other than those set forth in the Apparent Violations, or any activities that were the subject of OFAC's investigation.

70. OFAC may, in its sole discretion, post on OFAC's website this entire Agreement and/or issue a public statement about the facts of this Agreement, including the identity of any entities involved, the settlement amount, and a brief description of the Apparent Violations.

71. This Agreement consists of 18 pages, and expresses the complete understanding of OFAC and Respondent regarding resolution of OFAC's enforcement matter involving the Apparent Violations. No other agreements, oral or written, exist between OFAC and Respondent regarding resolution of this matter.

72. This Agreement shall inure to the benefit of and be binding on each party, as well as its respective successors or assigns.

Respondent accepts the terms of this Settlement Agreement this 8 day of April, 2019

Torry Berntsen
CEO, Americas, and Regional Head CIB
Standard Chartered Bank

Date: April 9, 2019

Andrea Gacki
Director
Office of Foreign Assets Control