UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

RYAN BOWMAN and SANDRA BOWMAN, Plaintiffs, -against- HSBC HOLDINGS PLC, HSBC BANK PLC, HSBC BANK MIDDLE EAST LIMITED, HSBC BANK USA, N.A., BARCLAYS BANK, PLC, STANDARD CHARTERED BANK, ROYAL BANK OF SCOTLAND, N.V., CREDIT SUISSE AG, BANK SADERAT PLC, COMMERZBANK AG, and JOHN DOES 1-50, Defendants.	**AMENDED COMPLAINT** **JURY TRIAL DEMANDED** **Case No. 19-cv-2146 (PKC)(CLP)**

TABLE OF CONTENTS

Plaintiffs, by their attorneys, allege the following:

I. NATURE OF THE ACTION

1. Running a decades-long terror campaign that claimed the lives of hundreds of Americans while simultaneously trying to complete a clandestine Weapons of Mass Destruction ("WMD") program is an extremely expensive proposition requiring access to billions of U.S. dollars ("USD"), including dollar-denominated assets in the Eurodollar market.[1]

2. For the Islamic Republic of Iran ("Iran") this was especially challenging since Iran's domestic currency, the Rial, was one of the world's least valued currencies, and was essentially worthless for purposes of global trade and commerce, including facilitating Iran's oil and natural gas exports, terror financing, conventional weapons trade, and WMD proliferation activities.

3. During the last eighteen years, while Western governments increased pressure against terrorism financing after Al Qaeda's September 11, 2001 attacks on the U.S. ("9-11"), Iran has intensified its efforts to access the U.S. financial system and U.S. export-controlled technologies, spare parts and raw materials while simultaneously evading U.S. sanctions, export restrictions and other laws and regulations intended to circumscribe its access to these capabilities and resources.

4. Fortunately for Iran—despite the coordinated and ever-intensifying efforts of the United States, the European Union and the United Nations after 9-11 to isolate Iran and restrict its capacity to fund terrorism and obtain WMD—it could rely upon an assortment of Western

[1] Eurodollar refers to a time deposit denominated in U.S. dollars that is maintained by a bank outside the United States. Payment transactions in the Eurodollar market are not typically settled by the physical transfer of USD-denominated banknotes from one counterparty to another. Instead, Eurodollar transactions are settled electronically in New York through a bank-owned clearinghouse, and then maintained by book entries of credits and debits in the respective counterparties' accounting systems (based on the Society for Worldwide Interbank Financial Telecommunication network ("SWIFT-NET") messages sent between the counterparties and their correspondent banks).

financial institutions willing to violate U.S. law to substantially assist its sanctioned endeavors.

5. Without the active and vital assistance of these Western financial institutions, Iran could not have conducted its terror campaign to nearly the same extent and magnitude, and it would have been severely hampered in its terror financing and WMD proliferation activities.

6. This is a civil action brought under 18 U.S.C. §§ 2333(a) and 2333 (d) of the Anti-Terrorism Act ("ATA") as a related action to *Freeman et al v. HSBC et al* (14-cv-6601 (PKC)(CLP)) and *Freeman et al v. HSBC et al* (18-cv-7359 (PKC)(CLP)) by Ryan Bowman, an American national, and his mother Sandra Bowman, also an American national for treble damages against seven Western international banks[2] that knowingly conspired with Iran and its banking agents (including Defendant Bank Saderat Plc, Bank Melli Iran, the Central Bank of Iran ("CBI"),[3] Bank Mellat, Bank Tejarat, Bank Refah and Bank Sepah) to evade U.S. economic sanctions, conduct illicit trade-finance transactions, and disguise financial payments to and from U.S. dollar-denominated accounts (the "Conspiracy").

7. The Conspiracy foreseeably enabled Iran and its agents to provide a combination of funding, weapons, munitions, intelligence, logistics, and training to the U.S.-designated Foreign Terrorist Organization ("FTO") Hezbollah; the U.S.-designated FTO Islamic Revolutionary Guard Corps ("IRGC"); the U.S.-designated FTO IRGC directorate known as the Islamic Revolutionary Guard Corps-Qods Force ("IRGC-QF"); and Iran's terrorist agents (including a litany of Iraqi Shi'a terror groups referred to herein collectively as the "Special Groups"), who injured Ryan Bowman in Iraq in April 2009, and his mother, Sandra Bowman.

---

[2] One of these seven, HSBC, technically comprises four banks: HSBC Holdings Plc; HSBC Bank Plc; HSBC Bank Middle East Ltd.; and HSBC Bank USA, N.A.

[3] CBI is occasionally referred to as Bank Markazi (spelled phonetically in a variety of ways).

8. In fact, on October 25, 2019, the United States issued its "Fifth Special Measure against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern" pursuant to Section 311 of the USA PATRIOT Act (Section 311 Designation").

9. The U.S. government found that "Iran has continued to evade these sanctions, fund terror and destabilizing activities, and advance its ballistic missile development" and that "Iran is a jurisdiction of primary money laundering concern." It also described the "illicit finance threat, including the terrorist-finance threat, that the jurisdiction of Iran poses to the United States and the U.S. financial system."

10. It confirmed that "Iran has developed covert methods for accessing the international financial system and pursuing its malign activities, including misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran (CBI)" and that "[t]hese efforts **often serve to fund the Islamic Revolutionary Guard Corps (IRGC), its Islamic Revolutionary Guard Corps Qods Force (IRGC-QF), Lebanese Hizballah (Hizballah),** Hamas, the Taliban and other terrorist groups." (Emphasis added.)

11. The Section 311 Designation further found that "Senior CBI officials have played a critical role in enabling illicit networks, using their official capacity to procure hard currency and conduct transactions for the benefit of the IRGC-QF and its terrorist proxy groups. The CBI has been complicit in these activities, including providing billions of U.S. dollars (USD) and euros to the IRGC-QF, Hizballah and other terrorist organizations."

12. The Section 311 Designation also reiterated that: "[i]n April 2019, the State Department designated the IRGC, including the IRGC-QF, as a Foreign Terrorist Organization (FTO). It was the first time that the United States designated a part of another government as an

FTO – an action that highlighted **Iran's use of terrorism as a central tool of its statecraft and an essential element of its foreign policy. The IRGC is integrally woven into the Iranian economy, operating institutions and front companies worldwide, so that the profits from seemingly legitimate business deals may actually fund Iranian terrorism.**" (Emphasis added.)

13. With respect to Bank Melli, the Section 311 Designation stated that:

> Bank Melli was among those banks designated pursuant to E.O. 13224 for assisting in, sponsoring, or providing financial, material, or technological support for, or other services to or in support of, the IRGC-QF. As of 2018, the equivalent of billions of USD in funds had transited IRGC-QF controlled accounts at Bank Melli. Moreover, Bank Melli had enabled the IRGC and its affiliates to move funds into and out of Iran, while the IRGC-QF, using Bank Melli's presence in Iraq, had used Bank Melli to pay Iraqi Shia militant groups.

14. The named Defendants herein are HSBC Holdings Plc, HSBC Bank Plc ("HSBC-London"), HSBC Bank Middle East Ltd., HSBC Bank USA, N.A. (referred to herein collectively as the "HSBC Defendants"); Barclays Bank Plc ("Barclays"); Standard Chartered Bank ("SCB"); Royal Bank of Scotland N.V. (referred to herein as "ABN Amro" or "RBS N.V."); Credit Suisse AG ("Credit Suisse"); Bank Saderat Plc; Commerzbank AG ("Commerzbank") and John Does 1-50.

15. Each Defendant committed acts of international terrorism and violated 18 U.S.C. § 2339A and § 2339B when it conspired to provide material support or resources, or concealed or disguised the nature, location, source, or ownership of material support or resources, (a) knowing or intending that they were to be used in preparation for, or in carrying out, a violation of 18 U.S.C. § 2332 and other federal crimes or (b) to FTOs Hezbollah and Kata'ib Hezbollah, knowing they were so-designated or had engaged in terrorist activity.

16. Each Defendant conspired to provide or conceal the source of material support by conspiring with Iran to evade U.S. economic sanctions and arms embargos against Iran knowing,

or deliberately indifferent to the fact, that Iran would use some of the funds[4] it laundered through the United States to finance the IRGC, IRGC-QF, and Hezbollah for the purpose of killing and maiming, *inter alia*, American citizens serving as part of the Coalition Forces in Iraq from 2004 to 2011.

17. As shown below, each Defendant conspired to provide material support by facilitating the transfer to the IRGC (designated an FTO on April 15, 2019), other Iranian entities, Hezbollah, and other designated entities and fronts for designated entities, of USD funds outside of the mechanism for Iran's legitimate agencies, operations, and programs.

18. As shown below, each Defendant conspired to conceal the source of material support by removing that information from transactional messages, as necessary to deceive U.S. counter-terrorism finance regulators.

19. The United States designated Iran a State Sponsor of Terrorism on January 19, 1984, pursuant to § 6(j) of the Export Administration Act, § 40 of the Arms Export Control Act, and § 620A of the Foreign Assistance Act. The designation has remained in effect since that time.

20. The United States designated Hezbollah an FTO (as that term is defined in 8 U.S.C. § 1189 of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA")) in 1997. The designation has remained in effect since that time.

21. In October 2007, the United States designated Iran's Ministry of Defense and Armed Forces Logistics ("MODAFL").

22. The U.S. government explained the basis for the designation as follows:

> The Ministry of Defense and Armed Forces Logistics (MODAFL) controls the Defense Industries Organization, an Iranian entity identified in the Annex to UN Security Council Resolution 1737 and designated by the

[4] USD funds include the following U.S. dollar-denominated financial instruments: deposit balances in domestic or Eurodollar bank accounts, repurchase agreements, letters of credit, bills of exchange, payment orders, checks, banknotes and coins.

> United States under E.O. 13382 on March 30, 2007. MODAFL also was sanctioned, pursuant to the Arms Export Control Act and the Export Administration Act, in November 2000 for its involvement in missile technology proliferation activities.
>
> MODAFL has ultimate authority over Iran's Aerospace Industries Organization (AIO), which was designated under E.O. 13382 on June 28, 2005. The AIO is the Iranian organization responsible for ballistic missile research, development and production activities and organizations, including the Shahid Hemmat Industries Group (SHIG) and the Shahid Bakeri Industries Group (SBIG), which were both listed under UN Security Council Resolution 1737 and designated under E.O. 13382. The head of MODAFL has publicly indicated Iran's willingness to continue to work on ballistic missiles. Defense Minister Brigadier General Mostafa Mohammad Najjar said that one of MODAFL's major projects is the manufacturing of Shahab-3 missiles and that it will not be halted. MODAFL representatives have acted as facilitators for Iranian assistance to an E.O. 13382-designated entity and, over the past two years, have brokered a number of transactions involving materials and technologies with ballistic missile applications.

23. Formally, the IRGC is a subordinate directorate of MODAFL, but in practice, it has substantial autonomy from MODAFL.

24. The IRGC, however, uses MODAFL to both procure and develop weapons and equipment for its use.

25. In October 2007, the United States designated the IRGC-QF a Specially Designated Global Terrorist ("SDGT") pursuant to Executive Order ("E.O.") 13324, explaining that:

> The Qods Force has had a long history of supporting Hizballah's military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support. The Qods Force operates training camps for Hizballah in Lebanon's Bekaa Valley and has reportedly trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran. The Qods Force provides roughly $100 to $200 million in funding a year to Hizballah and has assisted Hizballah in rearming in violation of UN Security Council Resolution 1701.
>
> *In addition, the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi'a militants who target and kill Coalition and Iraqi forces and innocent Iraqi civilians.* [Emphasis added.]

26. In October 2007, Defendant Bank Saderat Plc, together with its parent company Bank Saderat Iran, was designated an SDGT by the United States pursuant to E.O. 13224.

27. The U.S. Treasury Department's 2007 press release regarding Bank Saderat's designation stated:

> Bank Saderat, its branches, and subsidiaries: Bank Saderat, which has approximately 3200 branch offices, has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and EU-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad. For example, from 2001 to 2006, Bank Saderat transferred $50 million from the Central Bank of Iran through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence.

28. On October 12, 2011, the United States designated the Iranian commercial airline Mahan Air as an SDGT for "providing financial, material and technological support to the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF). Based in Tehran, Mahan Air provides transportation, funds transfers and personnel travel services to the IRGC-QF."

29. The Treasury Department explained Mahan Air's direct involvement with terrorist operations, personnel movements and logistics on behalf of the IRGC-QF:

> Mahan Air also facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel.
>
> Mahan Air crews have facilitated IRGC-QF arms shipments. Funds were also transferred via Mahan Air for the procurement of controlled goods by the IRGC-QF.
>
> In addition to the reasons for which Mahan Air is being designated today, Mahan Air also provides transportation services to Hezbollah [sic], a Lebanon-based designated Foreign Terrorist Organization. Mahan Air has transported personnel, weapons and goods on behalf of Hezbollah [sic] and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hezbollah [sic].

30. Mahan Air was also later identified as the conduit to Iran of *thousands* of radio frequency modules recovered by Coalition Forces in Iraq from Improvised Explosive Devices ("IEDs") that were used to target U.S. and Coalition Forces.

31. Hamid Arabnejad Khanooki, Mahan Air's chairman and CEO, is a former member of the IRGC and is a veteran of the same local IRGC division that spawned IRGC-Qods Force Commander Qasem Soleimani.

32. On May 31, 2013, the United States "designated . . . Mahan Air Managing Director Hamid Arabnejad who oversees Mahan Air's sanctions evasion efforts and provision of support and services to Iran's IRGC-QF."

33. On August 2, 2017, the Countering America's Adversaries Through Sanctions Act, Pub. L. 115-44, was enacted, in which Congress found that "The IRGC, not just the IRGC-QF, is responsible for implementing Iran's international program of destabilizing activities, support for acts of international terrorism, and ballistic missile program."

34. On October 13, 2017, the United States designated the IRGC an SDGT, finding that "The IRGC has played a central role to Iran becoming the world's foremost state sponsor of terror. Iran's pursuit of power comes at the cost of regional stability, and Treasury will continue using its authorities to disrupt the IRGC's destructive activities."

35. Specifically, the U.S. designated the IRGC as the "parent organization of the IRGC-QF," and "for the activities it undertakes to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, the IRGC-QF."

36. Further, the U.S found that the IRGC "undertakes to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, the IRGC-QF."[5]

37. As noted above, on April 15, 2019, the United States designated the IRGC an FTO. In designating the IRGC, the Department of State found that:

> The Iranian regime is responsible for the deaths of at least 603 American service members in Iraq since 2003. This accounts for 17% of all deaths of U.S. personnel in Iraq from 2003 to 2011, and is in addition to the many thousands of Iraqis killed by the IRGC's proxies.[6]

38. As used in this Complaint, "the Conspiracy" refers to an illegal criminal agreement, beginning in 1987 and, on information and belief, continuing to the present, between Iran, its banking agents and various international financial institutions by and through which Defendants knowingly participated in a criminal scheme in which they agreed to alter, falsify, or omit information from bank-to-bank payment orders sent on the SWIFT private financial messaging network ("SWIFT-NET") operated by the Society for Worldwide Interbank Telecommunication ("SWIFT-Brussels")[7] that involved Iran or Iranian parties (including several Iranian banks (referred to herein collectively as the "Iranian Bank Co-conspirators") such as Bank Melli Iran, Bank Saderat Iran, the CBI, Bank Mellat, Bank Tejarat, Bank Refah and Bank Sepah, as well as

---

[5] Although the IRGC-QF had responsibility for orchestrating Iranian policy in Iraq, including its terror campaign, as referenced herein, the IRGC and its operational directorate IRGC-QF are used interchangeably. As the U.S. government has found, the IRGC is the parent organization and principal supporter of the IRGC-QF.

[6] https://www.state.gov/designation-of-the-islamic-revolutionary-guard-corps/.

[7] SWIFT-Brussels is a cooperative society under Belgian law owned by its member financial institutions. SWIFT-Brussels's global private network, SWIFT-NET, enables financial institutions to send and receive information about financial transactions in the Eurodollar market, among other financial markets, in a standardized message format.

the Islamic Republic of Iran Shipping Lines ("IRISL"),[8] the National Iranian Oil Company ("NIOC") (an agent of the IRGC) and Mahan Air that serve as financial and logistical conduits for the IRGC and its terrorist activities.

39. The aims and objectives of the Conspiracy, all of which were intended and foreseeable to Defendants, and which each Defendant knew or was deliberately indifferent to, included, among others:

a. Concealing Iran's dollar-denominated financial activities and transactions from detection, scrutiny, or monitoring by U.S. regulators, law enforcement, and/or depository institutions;

b. Facilitating illicit transactions totaling at least $50 million USD for the benefit of Hezbollah;

c. Facilitating illicit transactions totaling at least $100 million in USD funds for the direct benefit of the IRGC and billions in USD funds for the benefit of NIOC, then controlled by the IRGC;

d. Facilitating at least hundreds of illicit transactions totaling more than $60 million on behalf of IRISL, including over 150 "stripped" transactions after IRISL was designated a Specially Designated National ("SDN");

e. Facilitating tens of millions of dollars in illicit transactions on behalf of MODAFL, the IRGC, Mahan Air and other instrumentalities of Iranian state-sponsored terror to further numerous violations of the U.S. trade embargo against Iran, conceal Iran's efforts to evade U.S. sanctions and enable Iran's acquisition from the United States of goods and technologies prohibited by U.S. law to be sold or transferred to Iran, including components of IEDs deployed against Coalition Forces in Iraq; and

f. Enabling Iran, the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc), the IRGC, Hezbollah, and their Special Groups proxies to plan for, conspire to, and perpetrate acts of international terrorism under 18 U.S.C. § 2331(1); homicides, attempted homicides, or conspiracies to commit homicide under 18 U.S.C. § 2332(a)-(c); bombings using destructive devices under 18

[8] IRISL is Iran's national maritime carrier: a global operator of merchant vessels with a worldwide network of subsidiaries, branch offices and agent relationships. It provides a variety of maritime transport services, including bulk, break-bulk, cargo and containerized shipping.

U.S.C. § 2332a; bombings and attempted bombings under 18 U.S.C. § 2332f; engaging in terrorist activity under 8 U.S.C. § 1189(a)(3)(B)(iii)-(iv); and/or engaging in terrorism under 22 U.S.C. § 2656f.

40. As noted by the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") in a March 20, 2008 advisory: "Through state-owned banks, the Government of Iran disguises its involvement in proliferation and terrorism activities through an array of deceptive practices specifically designed to evade detection."[9]

41. Although the Conspiracy was effectuated in a variety of ways, four primary techniques were used by Iran acting in concert with both the Iranian Bank Co-conspirators, MODAFL, the IRGC, IRISL and the Defendants herein:

a. The Defendants removed or altered the names, Bank Identifier Codes ("BICs"), and other identifying information of the Iranian Bank Co-conspirators or Iranian counter-parties in the payment orders sent through U.S. correspondent banks via SWIFT-NET– a practice commonly known and referred to as "stripping" SWIFT-NET messages;

b. The Defendants converted ordinary transactions involving SWIFT-NET message type 103 ("MT 103") payment orders (that would disclose the details of the counter-parties to the transactions) into bank-to-bank transfers known as SWIFT-NET message type 202 ("MT 202") payment orders (that did not require the transmitting bank to include information disclosing the originator, beneficiary, and counter-parties), for the specific purpose of concealing the origin and destination of Iranian funds transfers;

c. The Defendants deliberately chose not to conduct the required screening of Iran-linked SWIFT-NET messages[10] and letters of credit documents, worth at least tens of millions in USD funds on an annual basis, for compliance with the U.S. Office of Foreign Assets Control ("OFAC") list of SDNs; the U.S. State Department's United

[9] *See*, https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-a002.pdf.

[10] Including, but not limited to, SWIFT-NET messages for customer credit transfers ("MT 100" series messages), bank-to-bank transfers ("MT 200" series messages), foreign exchange ("MT 300" series messages), trade finance ("MT 400" and "MT 700" series messages), precious metals trading ("MT 600" series messages), and account management ("MT 900" series messages).

States Munitions List ("USML") of defense-related export controlled items; and/or the U.S. Bureau of Industry and Security's ("BIS") Commerce Control List ("CCL") of dual-use export controlled items, and Denied Persons List ("DPL") of export denied entities; and

d. The Defendants knowingly and willfully facilitated the illicit export and import of Iranian petroleum products for the NIOC (and hence for the IRGC) and other sanctioned Iranian entities. These petrodollar transactions, including trade-finance and foreign exchange, provided Iran with illegal access to billions of dollars, including the direct funding through the Defendants of the IRGC and its network of front companies.

42. Absent the criminal collusion and conspiratorial conduct of the Defendants named herein, Iran and its agents—including MODAFL, IRISL, the IRGC and the IRGC's agent, NIOC; and Banks Melli, Sepah, Refah, Mellat and Saderat—could not have successfully hidden the volume of U.S. dollar clearing and trade-finance transactions that they succeeded in illegally clearing through the United States in U.S. dollars.[11]

43. The connection between the IRGC, IRGC-QF and Bank Melli Iran, their "deceptive banking practices" and the attack that injured the Plaintiffs is further illustrated by a 2009 U.S. diplomatic cable which stated:

> *Iran's Islamic Revolutionary Guards Corps (IRGC) and IRGC-Qods Force, who channel funds to militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians, have used Bank Melli and other Iranian banks to move funds internationally.* Bank Melli used deceptive banking practices to obscure its involvement from the international banking system by requesting that its name be removed from financial transactions when handling financial transactions on behalf of the IRGC. [Emphasis added.]

[11] The Defendants willfully circumvented the sanctions screening, anti-money laundering ("AML"), and combatting the financing of terrorism ("CFT") requirements of OFAC, SWIFT-Brussels, Clearing House Interbank Payment System ("CHIPS-NY"), CLS Bank International ("CLS-NY"), Federal Reserve Bank of New York ("FRB-NY") and the Fedwire Funds Service ("Fedwire"). CHIPS is a Systemically Important Financial Market Utility ("SIFMU") for the U.S. financial system and the primary provider of clearing and settlement services in USD funds for Eurodollar transactions. CLS Bank is a Systemically Important Financial Market Utility ("SIFMU") for the U.S. financial system and the primary provider of clearing and settlement services for foreign exchange transactions in the Eurodollar market, and FRB-NY is one of the twelve U.S. Federal Reserve Banks and the central bank lender-of-last-resort for the Eurodollar market (via Fedwire).

44. This is further confirmed by the Section 311 Designation in October 2019, which noted that "[a]s of 2018, the equivalent of billions of USD in funds had transited IRGC-QF controlled accounts at Bank Melli. Moreover, Bank Melli had enabled the IRGC and its affiliates to move funds into and out of Iran, while the IRGC-QF, using Bank Melli's presence in Iraq, had used Bank Melli to pay Iraqi Shia militant groups."

45. Iran's objectives were not secret. Its pursuit and development of Weapons of Mass Destruction—including mines and similar explosive munitions—were the subject of hundreds of news reports, U.S. government reports, and Congressional testimony, as well as U.N. Security Council resolutions and European Union regulations.

46. Iran's "deceptive banking practices" were not secret either.

47. Beginning in September 2006, the U.S. Treasury and State Departments launched a quiet campaign to warn 40 major international banks and financial institutions about the risks of conducting business with the Iranian government, particularly targeting financial transactions involving the IRGC.

48. According to the March 26, 2007 edition of *The Washington Post*, Defendants Standard Chartered Bank, Commerzbank and the HSBC Defendants were among those briefed by U.S. government officials about the dangers posed (in terms of both proliferation and terror financing) in conducting business with Iran.

49. On April 19, 2007, the Wolfsberg Group, an association of twelve global banks whose stated aim is to develop financial services industry standards, issued a statement "endorsing measures to enhance the transparency of international wire transfers to promote the effectiveness of global anti-money laundering and anti-terrorist financing programs. The measures include both the development of an enhanced payment message format, which would include more detailed

information about those conducting wire transfers in certain instances, as well as calling for the global adoption of basic messaging principles aimed at promoting good practice with respect to the payment system." This statement was directed to the increasingly apparent risks inherent in MT 202 "cover payments" – one of the methods Defendants used to conceal their illegal USD funds transfers on behalf of Iran through the Eurodollar market.

50. Defendants ABN Amro (RBS N.V.), Barclays, Credit Suisse, and HSBC were all members of the Wolfsberg Group, and were listed on the 2007 press statement.

51. Iran's efforts to kill and maim U.S. and British citizens in Iraq, and to thwart U.S. policy objectives in Iraq, were also readily apparent and widely reported.

52. In fact, Iran's role in funding "militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians" was a matter of public record.

53. For example, on October 10, 2005, the British Broadcasting Company (BBC) reported that:

> An armour-piercing version of the bomb - blamed for the deaths of eight British soldiers this year - marks the latest advance in the insurgents' arsenal. *The UK has accused Iran of supplying the new weapon to militants in southern Iraq, via the Lebanese Hezbollah militia group,* although Tehran has denied this. [Emphasis added.]

54. The BBC followed up with multiple reports in 2006 describing the details from military briefings about Iran's material support to Shi'a militia groups that were targeting and killing British and U.S. forces in Iraq.

55. For example, on June 23, 2006, the BBC reported:

> BBC world affairs correspondent, Paul Reynolds, says both the American and British military in Iraq have claimed for some time that Iran, or factions within the Iranian government, have been supporting Shias politically and militarily.
>
> For example, the British ambassador to Baghdad William Patey accused the

> Iranian Revolutionary Guard of helping to supply the technology which has been used in bomb attacks against British troops in the south.
>
> "Since January we have seen an upsurge in their support, particularly to the Shia extremist groups," Gen Casey said.
>
> "They are using surrogates to conduct terrorist operations both against us and against the Iraqi people.
>
> "We are quite confident that the Iranians, through the special operations forces, are providing weapons, IED [improvised explosive device] technology and training to Shia extremist groups in Iraq," he said.

56. In another example, on September 26, 2008, CNN reported that U.S. officials claimed Iran had provided Shi'a militias in Iraq with "millions of dollars" in funding and that:

> The official said that high-grade military explosives and specialized timers are among the "boutique military equipment" moving from Iran into Iraq. Some of the equipment is of the same type that Hezbollah, an Iranian-backed Shiite militia, used against Israeli forces in Lebanon during the summer, the official said. The origin of the weapons was easy to discern because of Iranian markings on it, he said. Because Iran maintains tight control over armaments, he said, shipment of the weapons into Iraq had to involve "elements associated with the Iranian government."

57. Each of the Defendants knew about the existence of the Conspiracy; directly conspired with Iran, through Defendant Bank Saderat Plc, Bank Melli Iran, the CBI, the IRGC and others, to facilitate the Conspiracy; took affirmative, extensive and unlawful actions to further the Conspiracy over long periods of time; and was aware of the existence and participation of other Co-conspirators, including other Defendants named herein.

58. In fact, on numerous occasions, three or more of the Defendants acted jointly to facilitate the same illegal trade-finance transaction (*e.g.* providing material assistance to Mahan Air because the Iranian airline wanted to purchase U.S.-manufactured aircraft and needed help circumventing U.S. export restrictions against Iran).

59. Each of the Defendants, at the time it agreed to join and actively take part in the

Conspiracy, knew that Iran was a U.S.-designated State Sponsor of Terrorism and knew that Iran was clandestinely routing billions of dollars through the United States to hide its unlawful conduct; and each Defendant took affirmative steps to help Iran in its unlawful conduct.

60. Each of the Defendants also knew, or was deliberately indifferent to the fact, that Iran, as a U.S.-designated State Sponsor of Terrorism, would (and, in fact, did) channel hundreds of millions of the dollars that Defendants helped launder and conceal from U.S. regulators and law enforcement agencies to the IRGC and Hezbollah as part of the Conspiracy.

61. Each of the Defendants also knew, or was deliberately indifferent to, the well-publicized fact that Iran and its terror proxies were killing and maiming large numbers of American civilians and servicemen in Iraq, and that U.S. nationals would foreseeably be injured or killed as a result of the substantial assistance those dollars provided to the IRGC and Hezbollah.

62. Each of the Defendants also knew, or was deliberately indifferent to, the foreseeable (and inevitable) consequences of providing Iran, a State Sponsor of Terrorism, with access to hundreds of *billions* of dollars of concealed payments and the resulting funding of Iranian-controlled organizations and terror proxies that targeted American civilians and servicemen through acts of international terrorism in Iraq from 2004 to 2011.

63. Without the active participation of the Defendants in the Conspiracy, Iran could not have transferred the same volume of USD to the IRGC and Hezbollah, nor could it have done so with the same ease and efficiency.

64. Without the active participation of the Defendants in the Conspiracy, Iran could not have successfully violated U.S. export controls, financed its illicit arms shipments or manufactured the same volume and sophistication of factory-grade Explosively Formed Penetrators ("EFPs") to

kill and maim Americans in Iraq as discussed below.[12]

65. The transfers of hundreds of millions of dollars by Iran to the IRGC and Hezbollah was within the scope, and in furtherance of, the Conspiracy; and the provision of material support to the IRGC and Hezbollah was the natural and reasonably foreseeable consequence of the Defendants' unlawful agreement to help Iran clandestinely launder money through the United States financial system.

66. As set forth below, the HSBC Defendants, Commerzbank, Standard Chartered Bank, Barclays, and Credit Suisse altered, falsified, or omitted information from payment order messages that they facilitated on behalf of Bank Saderat knowing, or deliberately indifferent to the fact, that Bank Saderat was engaged in money laundering on behalf of a State Sponsor of Terrorism, and after October 2007, that Bank Saderat was an SDGT that provided material support to Iran's terrorist activities, and, in the case of the HSBC Defendants, knew there was direct evidence of Bank Saderat "funding of Hezbollah."

67. As set forth below, the HSBC Defendants, and Defendants Standard Chartered Bank, ABN Amro (RBS N.V.), and Commerzbank facilitated numerous payments totaling more than $60 million on behalf of IRISL knowing, or deliberately indifferent to the fact, that IRISL was designated an SDN by the United States for, as stated in the U.S. Treasury Department's

[12] EFPs are a particularly effective form of manufactured IED sometimes known as a shaped charge, usually made with a manufactured concave copper disk and a high explosive packed behind the liner. In Iraq, EFPs were often triggered by various technologies, including passive infra-red sensors (tripped by the engine heat of passing vehicles) and radio frequency modules (that would turn on the PIR before the high-powered radio waves generated by Coalition Forces' jamming devices could deploy). Metallurgic analysis by U.S. technicians helped confirm that the high-purity copper EFP liners were not produced in Iraq. Differences in the liners indicated the kind of press that was required to fabricate them—a heavy (hydraulic) press not commonly seen in Iraq. To produce these weapons, copper sheets were often loaded onto a punch press to yield copper discs. These discs were annealed in a furnace to soften the copper. The discs were then loaded into a large hydraulic press and formed into the disk-like final shape. This manufacturing process is critical to the design and concomitant lethality of the weapon. When the explosives inside an EFP detonate, the blast energy inverts the copper plate into a ragged slug traveling over a mile per second, capable of punching through armor even 300 feet away.

September 10, 2008 press release announcing IRISL's designation, "facilitating shipments of military cargo destined for the (Iranian) Ministry of Defense and Armed Forces Logistics (MODAFL)," which could be used for terrorist attacks on Coalition Forces, including American nationals.

68. IRISL *did*, in fact, facilitate shipments of military cargo to Hezbollah, one of the terrorist organizations responsible for acts of international terrorism that killed and injured American citizens in Iraq, including the Plaintiffs.

69. As alleged below, Defendants Standard Chartered Bank, Credit Suisse, Bank Saderat Plc and Commerzbank all altered, falsified, or omitted information from payment messages (worth billions of U.S. dollars) that they facilitated on behalf of NIOC, then an agent of the IRGC, knowing, or deliberately indifferent to the risk involved in rendering those payments without any transparency to U.S. regulators and law enforcement, and thereby directly providing the IRGC with access to billions of USD that it could move – undetected – through the global financial system.

70. As alleged below, Defendant Standard Chartered Bank also knowingly and actively financed and facilitated illegal trade-finance transactions worth hundreds of millions of dollars on behalf of MODAFL, the IRGC and various instrumentalities of Iranian state-sponsored terror, including companies working directly for Hezbollah and the IRGC-Qods Force.

71. Furthermore, as alleged below, Defendants HSBC Bank USA, N.A., Standard Chartered Bank, ABN Amro (RBS N.V.), and Commerzbank committed acts of international terrorism in violation of 18 U.S.C. § 2332d.

72. Defendant HSBC Bank USA, N.A. is a U.S. person that knowingly conducted financial transactions with Iran in the United States in violation of 18 U.S.C. § 2332d, and it was

reasonably foreseeable that Iran would provide material support to acts of international terrorism that killed and injured American citizens in Iraq.

73. Plaintiffs further allege that the U.S. branches of Defendants Barclays, Standard Chartered Bank, ABN Amro (RBS N.V.), and Commerzbank are U.S. persons that knowingly conducted financial transactions with Iran in the United States in violation of 18 U.S.C. § 2332d, and it was reasonably foreseeable that Iran would provide material support to acts of international terrorism that killed and injured American citizens in Iraq.

74. Each of the Plaintiffs was injured as a result of an act of international terrorism for which Iran and its state-controlled organizations and terrorism proxies, including the IRGC and Hezbollah, were responsible.

II. JURISDICTION AND VENUE

75. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. §§ 2333(a) and 2338 as a civil action brought by citizens of the United States and/or their estates, survivors, or heirs, who have been injured by reason of acts of international terrorism.

76. Venue is proper in this district pursuant to 18 U.S.C. § 2334(a) and 28 U.S.C. §§ 1391(b) and 1391(d).

77. Defendants are subject to personal jurisdiction in the United States pursuant to 18 U.S.C. § 2334(a), CPLR § 302, and Fed. R. Civ. P. 4(k)(1)-(2). Defendant HSBC Bank USA, N.A. is also subject to personal jurisdiction under CPLR § 301. Defendants' unlawful conduct was purposefully directed at the United States, and the Conspiracy was specifically designed to effectuate the flow of billions of USD through the United States in violation of U.S. laws, and in fact resulted in hundreds of billions of dollars illegally passing through the United States.

III. THE PLAINTIFFS

1. THE APRIL 13, 2009 ATTACK

The Bowman Family

78. Plaintiff Ryan Bowman is a citizen of the United States and domiciled in the State of Pennsylvania.

79. On April 13, 2009, Ryan Bowman, then 23, was serving in the U.S. military in Iraq when the Chinook helicopter he was traveling in was attacked with an RPG-29 fired by Special Groups terror operatives.

80. Those operatives were trained by Hezbollah and funded and supplied by the IRGC-QF and they launched the attack at the direction of both Hezbollah and the IRGC-QF as their proxy.

81. At the time of the attack, Ryan Bowman was not clipped in to the Chinook helicopter. When the pilot of the Chinook helicopter took evasive actions to avoid the RPG-29, Mr. Bowman bounced around the helicopter suffering a TBI and permanent injury to his back.

82. Mr. Bowman has been determined to be 100% disabled by the Veterans Administration.

83. As a result of the attack, and the injuries he suffered, Plaintiff Ryan Bowman has experienced severe physical and mental anguish and extreme emotional pain and suffering.

84. Plaintiff Sandra Bowman is a citizen of the United States and domiciled in the State of Pennsylvania.

85. As a result of the attack and the injuries to Ryan Bowman, Plaintiff Sandra Bowman has experienced severe mental anguish and extreme emotional pain and suffering.

IV. THE DEFENDANTS

A. THE HSBC DEFENDANTS

86. Defendant HSBC Holdings Plc ("HSBC Holdings") is a public limited company organized under the laws of the United Kingdom. HSBC Holdings directly or indirectly owns, *inter alia*, Defendant HSBC Bank Plc, Defendant HSBC Bank Middle East Limited, and Defendant HSBC Bank USA, N.A. (as noted above, referred to herein collectively as the "HSBC Defendants"). HSBC Holdings is occasionally referred to internally (and in this Amended Complaint) as "HSBC Group," or "The Group," and members and affiliates of HSBC Holdings (including the named HSBC Defendants herein) are occasionally referred to herein as "HSBC Group members."

87. Defendant HSBC Holdings constitutes the ultimate parent company of one of the world's largest banking and financial services groups with approximately 6,300 offices in over 75 countries and territories.

88. HSBC Holdings is listed on the New York Stock Exchange ("NYSE"), London Stock Exchange ("LSE") and Hong Kong Stock Exchange ("SEHK").

89. HSBC Group members comprise financial institutions throughout the world that are owned by various intermediate holding companies, and ultimately, but indirectly, by Defendant HSBC Holdings, which, as alleged above, is incorporated and headquartered in England.

90. Defendant HSBC Bank Plc ("HSBC-London," often referred to internally by members of HSBC Group as "HBEU") is a financial institution registered under the laws of England and Wales.

91. Defendant HSBC Bank Middle East Limited ("HSBC-Middle East," often referred to internally by members of HSBC Group as "HBME"), is a financial institution registered under

the laws of the Jersey Channel Islands.

92. Defendant HSBC Bank USA, N.A. ("HSBC-US," often referred to internally by members of HSBC Group as "HBUS"), is a national bank chartered under the National Bank Act (12 U.S.C. § 2 *et seq*.) that constitutes a "U.S. person" under the definitions set forth in 31 C.F.R. Part 560.314 of the Iranian Transactions Regulations (the "ITR") and 18 U.S.C. § 2332d(b)(2) of the Anti-Terrorism Act ("ATA").

93. According to the fact sheets published on HSBC-US's official website, HSBC-US's headquarters are in McLean, VA, and it has its principal office in New York City.

94. HSBC-US operates more than 240 bank branches throughout the United States, with offices and branches in New York, California, Connecticut, Delaware, Washington, D.C., Florida, Maryland, New Jersey, Oregon, Pennsylvania, Virginia, and Washington State.

95. HSBC-US is the principal subsidiary of HSBC USA Inc., which is, in turn, an indirect, wholly owned subsidiary of HSBC North America Holdings, Inc. ("HNAH"). HNAH's businesses serve customers in retail banking and wealth management, commercial banking, private banking, and global banking and markets.

B. DEFENDANT BARCLAYS BANK PLC

96. Defendant Barclays Bank Plc ("Barclays") is a global financial services provider headquartered in London, United Kingdom.

97. Defendant Barclays is a wholly owned subsidiary of Barclays Plc, a public limited liability company organized under the laws of England and Wales.

98. As used in this Amended Complaint, "Barclays" refers to Barclays Bank Plc, the wholly owned subsidiary of Barclays Plc, not Barclays Plc, Defendant Barclays Bank Plc's parent company.

99. Barclays is one of the largest banks in the world. Barclays' home country regulator is the United Kingdom's Financial Services Authority ("FSA").

C. DEFENDANT STANDARD CHARTERED BANK

100. Defendant Standard Chartered Bank ("SCB") is one of the world's largest international banks, with over 1,700 branches, offices, and outlets in more than 70 countries. Headquartered in London, SCB operates principally in Asia, Africa, and the Middle East, and has operations in consumer, corporate and institutional banking, and treasury services.

101. SCB-London is listed on the London Stock Exchange ("LSE") and Hong Kong Stock Exchange ("SEHK").

102. Since 1976, SCB has had a license issued by the state of New York to operate as a foreign bank branch in New York, New York ("SCB-NY"). The branch provides wholesale banking services, primarily U.S.-dollar clearing for international wire payments.

103. Standard Chartered's New York branch is the seventh largest U.S. dollar correspondent bank in the world, clearing and settling approximately 195 billion in USD funds per day.

104. Standard Chartered's New York branch also constitutes a "U.S. person" under the definitions set forth in § 560.314 of the ITR and 18 U.S.C. § 2332d(b)(2).

D. DEFENDANT ROYAL BANK OF SCOTLAND N.V.

105. In October 2007, a consortium consisting of Fortis, the Royal Bank of Scotland Group ("RBS"), and Banco Santander acquired ABN Amro Holding N.V., the parent company of ABN Amro Bank N.V., using the acquisition vehicle RFS Holdings.

106. The former ABN Amro Bank N.V. subsequently underwent a restructuring process to transfer its Dutch State-acquired businesses and activities out of the existing ABN Amro Group.

To do so, the relevant Dutch State-acquired businesses were first transferred to a new legal entity owned by ABN Amro Holding N.V.

107. On February 5, 2010, through a statutory demerger process, the former ABN Amro Bank N.V. was renamed RBS N.V. In 2018, RBS N.V. was renamed NatWest Markets N.V.

108. Ultimately, RBS acquired ABN Amro Holding N.V. As such, RBS acquired the New York and Chicago branches of ABN Amro Bank N.V. and began integrating certain business lines handled by these branches into its other U.S. operations. These former branches constitute a "U.S. person" under the definitions set forth in § 560.314 of the ITR and 18 U.S.C. § 2332d(b)(2).

109. In this Amended Complaint, "ABN Amro (RBS N.V.)" refers to the named Defendant herein.

E. DEFENDANT CREDIT SUISSE AG

110. Defendant Credit Suisse AG ("Credit Suisse") is a financial services company headquartered in Zurich, Switzerland. Its U.S. headquarters are located at 11 Madison Avenue, New York, New York.

111. Credit Suisse serves clients worldwide through its Private Banking unit, which includes a Wealth Management and Corporate & Institutional Clients unit; Investment Banking unit; and Asset Management unit.

112. According to the CHIPS-NY website, Credit Suisse used the following U.S. financial institutions in New York to clear and settle its Eurodollar transactions:

a. Defendant HSBC Bank USA, N.A. (identified by CHIPS-NY participant number 0108 and Fedwire routing number 021001088);

b. The Bank of New York Mellon (identified by CHIPS-NY participant number 0001 and Fedwire routing number 011001234);

c. Deutsche Bank Trust Co Americas (identified by CHIPS-NY

participant number 0103 and Fedwire routing number 021001033); and

d. Wells Fargo Bank NY International (identified by CHIPS-NY participant number 0509 and Fedwire routing number 026005092).

113. Credit Suisse's New York branch is subject to oversight and regulation by the Board of Governors of the U.S. Federal Reserve System and the New York State Banking Department. The branch thus constitutes a "U.S. person" under the Iranian Transaction Regulations and § 2332d(b)(2).

F. DEFENDANT BANK SADERAT PLC

114. Bank Saderat Iran is one of the largest banks in Iran. It has approximately 3,400 offices worldwide, including, as discussed below, a United Kingdom subsidiary (Defendant Bank Saderat Plc), and branches in Frankfurt, Paris, Athens, Dubai and Beirut.

115. Bank Saderat Iran was nationalized after the Iranian Revolution, but allegedly privatized in 2009. According to Bank Saderat Iran, 49% of its shares are owned by the Iranian government, but it is technically a non-governmental entity.

116. In 2002, Bank Saderat Iran's London bank branch became a wholly owned bank subsidiary, incorporated under United Kingdom law (*i.e.* Defendant Bank Saderat Plc).

117. Bank Saderat Plc is the legal successor in interest to the Iran Overseas Investment Bank ("IOIB"), London.

118. IOIB changed its name to Bank Saderat Plc in March 2002.

119. Defendant Bank Saderat Plc maintains its principal office in London, United Kingdom.

G. DEFENDANT COMMERZBANK AG

120. Defendant Commerzbank AG ("Commerzbank") is a financial services company

headquartered in Frankfurt, Germany, and has over 1,200 branches in Germany alone.

121. According to the CHIPS-NY website, Commerzbank AG used, *inter alia,* the following U.S. financial institutions in New York to clear and settle its Eurodollar transactions:

a. Defendant Commerzbank's New York branch (identified by CHIPS-NY participant number 0804 and Fedwire routing number 026008044);

b. Defendant HSBC Bank USA, N.A. (identified by CHIPS-NY participant number 0108 and Fedwire routing number 021001088);

c. Defendant SCB-NY (identified by CHIPS-NY participant number 0256 and Fedwire routing number 026002561); and

d. Deutsche Bank Trust Co Americas (identified by CHIPS-NY participant number 0103 and Fedwire routing number 021001033).

122. Commerzbank maintains 23 foreign branches, including a New York branch licensed by the State of New York since 1967.

123. The New York branch of Commerzbank constitutes a "U.S. person" under the Iranian Transaction Regulations and § 2332d(b)(2).

124. Commerzbank is listed on stock exchanges in Germany, London, and Switzerland.

125. Defendants Barclays, Standard Chartered Bank, ABN Amro (RBS N.V.), Credit Suisse, Commerzbank, and the HSBC Defendants are sometimes referred to herein collectively as "the Western Bank Defendants."

V. FACTUAL ALLEGATIONS

A. IRAN'S LONG HISTORY OF SUPPORTING AND FINANCING TERRORISM

126. Since the Iranian Revolution in 1979, Iran has been a principal source of extremism and terrorism throughout the Middle East and the rest of the world, responsible for bombings, kidnappings and assassinations across the globe.

127. As noted above, the United States designated Iran a State Sponsor of Terrorism on January 19, 1984. That designation has remained in force throughout the relevant time period to this Action.

128. Since its 1984 designation, the United States has attempted to constrain and deter Iran's sponsorship and commission of terrorist activities, as well as its development of Weapons of Mass Destruction, by imposing a wide variety of trade and economic sanctions intended to reduce the flow of financial resources, especially U.S. dollar-denominated assets, for Iran's support of such activities.

B. U.S. SANCTIONS AND IRAN'S RELIANCE ON U.S. DOLLARS

129. On June 25, 1996, a truck bomb decimated a building at the Khobar Towers complex in Saudi Arabia that was used to house American military personnel, killing 19 Americans and wounding another 372 people.

130. It was soon established that the terrorist operatives responsible for the bombing were trained and equipped by the IRGC.

131. Soon thereafter, Congress responded by passing the 1996 Iran-Libya Sanctions Act finding that:

> (1) The efforts of the Government of Iran to acquire weapons of mass destruction and the means to deliver them *and its support of acts of international terrorism* endanger the national security and foreign policy interests of the United States and those countries with which the United States shares common strategic and foreign policy objectives.
>
> (2) The objective of preventing the proliferation of weapons of mass destruction and *acts of international terrorism* through existing multilateral and bilateral initiatives *requires additional efforts to deny Iran the financial means* to sustain its nuclear, chemical, biological, and missile weapons programs. [Emphasis added.]

132. To ensure that U.S. financial institutions that process international wire transfers in the Eurodollar market do not assist Iran in its support of international terrorism and weapons proliferation or facilitate other prohibited transactions, U.S. financial institutions have been (and are) required to use sophisticated computer systems and software algorithms to monitor and screen all wire transfer activities.

133. Banks in New York that process most of the world's Eurodollar payments and foreign exchange transactions depend on these automated systems to prevent Iran and other sanctioned entities (as well as terrorists, money launderers, and other criminals) from gaining access to the United States banking system. In this way, U.S. financial institutions are supposed to be the first line of defense to prevent Iran from accessing the U.S. financial system to fund or otherwise engage in terrorism and other prohibited conduct.

134. At the same time, because, on average, 60 percent of Iranian government revenues and 90 percent of Iran's export revenues originate from the sale of its oil and gas resources, a market largely denominated in USD (known as "petrodollars"[13]), and because Iran's currency, the Rial, was (in part due to U.S. sanctions) one of the world's least valued currencies, the Iranian regime was desperately dependent on access to the USD funds it maintained in the Eurodollar market, and the interest income these petrodollar deposits generated.[14]

135. Thus, reliably consistent access to, and the ability to facilitate trade in, the Eurodollar market has been critical to the capacity of the Iranian regime to fund its terror proxies such as Hezbollah in Lebanon, and to fuel its other terrorism and weapons proliferation activities through the IRGC.

---

[13] The petrodollar market developed because, *inter alia*, the United States was the largest producer and consumer of oil in the world; the world oil market has been priced in USD since the end of World War II.

[14] The Eurodollar interest rate is also known as the London Interbank Offered Rate ("LIBOR").

136. The importance to Iran of funding Hezbollah, the IRGC and subsequently, Kata'ib Hezbollah and other Special Groups in Iraq, became even more acute after the 2003 U.S. invasion of Iraq. After that event, Iran directed Hezbollah to create "Unit 3800" (discussed below) and began devoting greater financial resources to gain influence in Iraq, inflict casualties on American citizens in Iraq, and intensify its quest for Weapons of Mass Destruction.

137. *None* of these goals could be accomplished by Iran without USD funds, access to the Eurodollar market, and the agreement of Western financial institutions, such as the Western Bank Defendants, to shield Iran's unlawful Eurodollar and trade-finance activities from detection.

C. IRAN CONTINUOUSLY EVADED U.S., EUROPEAN UNION AND UNITED NATIONS SANCTIONS

138. Congress and successive Administrations have enacted several laws and executive orders that imposed sanctions on countries and firms that sell Weapons of Mass Destruction technology and military equipment to Iran.

139. On March 16, 1995, as a result of Iranian sponsorship of international terrorism and Iran's active pursuit of Weapons of Mass Destruction, President Clinton issued Executive Order 12957 prohibiting U.S. involvement with petroleum development in Iran.

140. On May 6, 1995, President Clinton signed Executive Order 12959, pursuant to the International Emergency Economic Powers Act ("IEEPA"),[15] as well as the 1985 International Security and Development Cooperation Act ("ISDCA"), substantially tightening sanctions against Iran.

[15] On October 16, 2007, President Bush signed into law the International Emergency Economic Powers (IEEPA) Enhancement Act, Public Law No. 110-96, amending IEEPA section 206. The Act enhanced criminal and administrative penalties that could be imposed under IEEPA.

141. On August 19, 1997, President Clinton signed Executive Order 13059 clarifying Executive Orders 12957 and 12959 and confirming that virtually all trade and investment activities with Iran by U.S. persons, wherever located, were prohibited.

142. In order to thwart U.S. sanctions efforts, Iran cultivated close relationships with foreign arms suppliers, including Russia, China, and North Korea.

143. In addition, Iran sought to clandestinely acquire dual-use technologies from European manufacturers, and certain export-controlled defense products, aircraft parts, dual-use technologies and materials from the United States.

144. For years, U.S. law enforcement officials, customs agents and intelligence services have worked to thwart Iranian efforts to circumvent U.S. economic sanctions and arms embargos.

145. A few brief examples illustrate the larger U.S. government effort:

- On March 12, 2001, criminal and civil sanctions were imposed on Refinery Industries, Inc., of Budd Lake, New Jersey, for attempted exports of gas detection equipment to Iran.

- On June 11, 2001, Saeed Homayouni and Yew Leng Fung, officials of Multicore, Inc., pled guilty in the U.S. in connection with the firm's purchase of commercial and military aircraft parts and missile components for export to Iran.

- In March 2007, the U.S. led efforts to pass U.N. Security Council Resolution 1747 that declared: "Iran shall not supply, sell or transfer directly or indirectly from its territory or by its nationals or using its flag vessels or aircraft any arms or related materiel."

- In March 2008, the U.S. led efforts to pass U.N. Security Council Resolution 1803 that called upon all member states "to exercise vigilance over the activities of financial institutions in their territories with all banks domiciled in Iran, in particular with Bank Melli and Bank Saderat, and their branches and subsidiaries abroad" and "to inspect the cargoes to and from Iran, of aircraft and vessels, at their airports and seaports, owned or operated by Iran Air Cargo and Islamic Republic of Iran Shipping Line, provided there are reasonable grounds to believe that the aircraft or vessel is transporting [prohibited] goods…"

- On September 17, 2008, the U.S. Department of Justice unsealed a criminal indictment against 16 foreign-based defendants related to Mayrow General Trading Company, for their involvement in providing Weapons of Mass Destruction-related, military, and dual-use items to Iran, specifically components found in IEDs in Iraq that caused deaths and injuries to U.S. military personnel.

- On December 11, 2009, at the request of the U.S. government, the Thai government detained a Russian aircraft containing a cargo of weapons from North Korea destined for Iran.

- On June 23, 2010, the U.S. Department of Justice charged an Iranian company and citizen, as well as Opto Electronics PTE, Ltd., a Singapore company and others with, *inter alia*, violations of the Arms Export Control Act (22 U.S.C. § 2778) for facilitating the unlawful transfer of long range radio frequency modules used in IEDs targeting Coalition Forces in Iraq. The modules were flown to Iran by Mahan Air.

- On May 11, 2010, Balli Aviation Ltd., a subsidiary of the U.K.-based Balli Group Plc., was sentenced in the District of Columbia to pay a $2 million fine, and to serve a five-year corporate period of probation after pleading guilty to a two-count criminal information in connection with its illegal export of a commercial Boeing 747 aircraft from the United States to Iran.

- In December 2012, the U.S. Department of Justice charged Business Machinery World Wide, an Iranian corporation based in Tehran, Iran; three of its subsidiary companies located in Dubai, United Arab Emirates; and nine officers and individuals for conspiring to violate the IEEPA by facilitating the shipment of computers to the United Arab Emirates for delivery to Iran.

- In April 2014, John Alexander Talley was sentenced to 30 months in prison for conspiracy to violate the IEEPA and Iranian Transaction and Sanctions Regulations. Talley's company, Tallyho Peripherals, Inc., was also sentenced to one year of probation. According to court documents, from 2009 to September 2012, Talley and his company conspired with others to unlawfully export sophisticated computer equipment from the United States to Iran. The shipments of the computers and the payments transited through the United Arab Emirates.

146. In addition, both the U.S. Treasury Department and Commerce Department have blacklisted a long list of Iranian front companies, shell companies and middlemen that the U.S. has determined to be complicit in Iran's sanctions evasion efforts.

D. THE EURODOLLAR MARKET – IRAN'S MONEY LAUNDERING AND ILLICIT EXPORT NEXUS WITH DEFENDANT BANKS

1. The Conspiracy's Shared Goals

147. As noted *supra*, Iran needed access to the Eurodollar market in order to sustain the Islamic Revolutionary government that has ruled Iran since 1979.

148. Specifically, the Government of Iran used the Eurodollar market for the following economic activities:

a. Investing petrodollar (in USD funds) revenue from Iran's oil and gas export sales;

b. Exporting the Iranian Islamic Revolution through acts of international terrorism; and

c. Illicitly acquiring U.S.-manufactured equipment, parts and technology to further its nuclear and conventional weapons programs.

149. Iran did not have a legitimate need to access the Eurodollar market for the benefit of any Iranian civilian agency, operation or program; it could have operated with funds denominated in any number of other Eurocurrencies[16] (deciding, instead, to continually conduct its international trade primarily in Eurodollars).

150. Specifically, Iran did in fact have access to viable alternative options both for foreign exchange and time deposits in Eurocurrencies (other than Eurodollars) to meet the needs

[16] The term Eurocurrency refers to deposits of funds transferred to, and maintained by, banks outside of the home country for the respective currency. Thus, had Iran chosen to convert its petrodollars into Japanese Yen, it would have held "Euroyen" deposits at banks outside of Japan.

of its civilian programs, including, but not limited to, its credit at the European Central Bank denominated in Euros, its credit at the International Monetary Fund ("IMF") denominated in Special Drawing Rights ("SDRs"), its credit at the Asian Clearing Union ("ACU") denominated in Asian Monetary Units ("AMUs"), or its domestic credit denominated in Iranian Rial.

151. However, Iran would not have been able to move its funds undetected through the Eurodollar market without the covert operational and technical assistance it received from the Defendants.

152. Likewise, Iran would not have been able to substantially fund Hezbollah and Shi'a militias in Iraq—and acquire U.S.-manufactured products (including dual-use technologies and export-controlled manufacturing equipment)—without access to USD funds through the Eurodollar market.

153. As a result of Iran's deceptive and illegal banking practices, Iran's access to the Eurodollar market through the Defendant Banks was cut-off by SWIFT-Brussels in mid-2012.

154. Soon thereafter, Iran's domestic currency collapsed.

155. The CBI was forced to intensify the use of its gold reserves in order to prop-up the Rial's value.

156. Absent the Defendant Banks providing Iran and its proxies with decades of clandestine access to the Eurodollar market, Iran's foreign policy goal of furthering its Islamic Revolution through the financing of terrorism—including Iran's sponsorship of terrorist attacks against Coalition Forces in Iraq between 2004 and 2011—would have been severely constrained.

2. Eurodollar Market Operations

157. As mentioned above, the global Eurodollar market is a wholesale, bank-to-bank market where a correspondent network of banks, bank branches and other bank affiliates outside

the United States make loans and accept deposits denominated in U.S. dollars.

158. According to the FRB-NY, the Eurodollar market emerged after World War II due to a large increase in U.S. dollars funds circulating outside of the United States from, *inter alia*, the Marshall Plan expenditures to rebuild Europe after the war.

159. Prior to the launch of SWIFT-NET in 1977, most transactions in the Eurodollar market were conducted electronically by telegraphic transfer ("TELEX").

160. By the time of the 1979 Iranian Revolution, the Bank of International Settlements ("BIS-Basel") estimated that the size of the Eurodollar market was over $600 billion.

161. A mid-2015 report by the Bank of International Settlements ("BIS-Basel") estimated that the size of the Eurodollar market by the end of 2014 was over twenty-one *trillion* in USD funds.

162. As mentioned *supra*, nearly all U.S. dollar transfers initiated through banks outside the United States are processed electronically by correspondent banks in the United States, almost exclusively in New York.

163. The Clearing House Interbank Payment System ("CHIPS-NY") represents that it processes 95 percent of those Eurodollar funds transfers.

E. THE IRANIAN U-TURN EXEMPTION AND ITS REVOCATION

164. Alongside its economic sanctions against Iran, the United States government designed an exception process to permit Iran's circumscribed access to U.S. dollars through a narrowly tailored exemption to the Iranian Trade Regulations, known as the "U-Turn exemption" (Section 560.516 of the Iranian Trade Regulations). At the same time, the U.S. government insisted that U.S. financial institutions operating in the Eurodollar market carefully monitor all Iranian

transactions to both deter and detect the financing of sanctioned entities involved in, *inter alia*, Iran's terrorism and weapons proliferation activities.

165. The purpose of the U-Turn exemption was to permit Iranian parties indirect access to USD funds, *provided* that these transactions were fully disclosed to U.S. correspondent banks; were strictly for Iran's legitimate agencies, operations and programs; and were not earmarked for terrorist, WMD proliferation or other proscribed purposes.

166. Until November 2008, U.S. financial institutions were authorized to process certain funds transfers (under the U-Turn exemption) for the direct or indirect benefit of Iranian banks, other persons in Iran or the Government of Iran, *provided* such payments were initiated offshore by a *non-Iranian*, non-U.S. financial institution and only passed through the U.S. financial system *en route* to another offshore, *non-Iranian*, non-U.S. financial institution; *and* provided that none of the parties to the transactions had been designated an SDN, or that the transaction was for an SDN's benefit.

167. The U-Turn exemption was therefore conditioned on transparency to permit the careful monitoring of all Iranian transactions, both to deter and detect terror financing and weapons proliferation activities.

168. Because so much of Iran's international trade has historically flowed through the United States for clearing and settlement and because Iran's primary terrorist proxy, Hezbollah, operates in Lebanon (itself a dollarized economy and largely dependent on U.S. currency) maintaining transparency in processing Iranian USD transactions has been a vital part of the architecture of U.S. national security for decades and was reflected as such in the Iranian Trade Regulations.

169. Iran's access through the U-Turn exemption was to be closely monitored filtering

all U-Turn exemption transactions through sophisticated computer systems used by U.S. financial institutions to monitor and screen all USD-denominated wire transfers.

170. The Western Bank Defendants, however, knowingly and intentionally agreed to, and did, manipulate tens of thousands of payment order messages (SWIFT-NET MT 103 and MT 202) and the records of such transactions to defeat such monitoring and screening, and prevent transparency, in order to provide USD funds to Iran for unlawful uses, which foreseeably included the support of Iranian terrorism and terrorist organizations.

171. Over time, however, U.S. authorities began to understand the contours of the Conspiracy involving Iran and the Defendants that is set forth in this Amended Complaint.

172. Initially, the realization that Iran was engaging in "deceptive banking practices" led the U.S. to target key Iranian financial institutions, entities, and individuals under proliferation, counterterrorism, and Iran-related sanctions (*i.e.*, E.O. 13382, E.O. 13224, and E.O. 13438, respectively).

173. The apparent assumption made initially by U.S. authorities was that Iran and its banking agents (Iranian Bank Co-conspirators Bank Sepah, Bank Melli, Bank Saderat and others) were engaged in deception that was exploiting unwitting Western financial institutions that were engaged in high risk but legal, foreign exchange, precious metals, and trade-finance business with Iran.

174. The truth was otherwise.

175. *First*, despite Iran's feeble domestic economy during the entire relevant period of time, its oil and natural gas exports still provided the Iranian regime with substantial revenues denominated in U.S. dollars.

176. *Second*, Iran's petrodollar revenues were managed by, and through, among others, the Central Bank of Iran ("CBI") and the Iranian Ministry of Petroleum (including NIOC; later designated an SDN pursuant to E.O. 13382 and identified as an agent or affiliate of the IRGC).[17]

177. *Third*, the challenge Iran faced was that it was almost entirely dependent on USD funds, but U.S. economic sanctions—and the attendant monitoring of Iran's financial activities—were incompatible with its terror financing and Weapons of Mass Destruction proliferation goals.

178. *Fourth*, between 2004 and 2011, both Lebanon (where Iran's agent, Hezbollah, is based) and Iraq (where Iran's proxies were launching terror attacks killing and injuring U.S. service members, including Ryan Bowman,) were U.S.-dollarized economies, a fiscal reality that made Iran's funding of its terror proxies a highly "dollar-sensitive" endeavor.

179. *Fifth*, in order to free itself from U.S. economic sanctions, and circumvent the U.S., European Union ("EU") and United Nations ("U.N.") monitoring of its financial activities, Iran needed more than a single willing partner among Western financial institutions to assist its illegal goals.

180. *Finally*, Iran needed the active assistance of at least *several* of the world's *largest* (non-U.S.) multinational banks that were already accustomed to handling large volumes of dollar clearing and settlement transactions, and thus would be less likely to raise suspicions with U.S. authorities.

181. For example, in early 2001, the Central Bank of Iran asked Defendant Standard Chartered Bank to act as its correspondent bank with respect to Iranian petrodollar payments, trade-finance and foreign exchange transactions on behalf of NIOC.

---

[17] That designation was removed in January 2016.

182. As set forth *infra*, Standard Chartered Bank agreed to participate in the Conspiracy and deliberately removed identifying data on NIOC's payment orders (SWIFT-NET MT 103 and MT 202 payment order messages) for these and other wire transfers.

183. The sheer size and volume of these NIOC transactions would have raised numerous red flags if not undertaken by a bank of SCB's size and existing USD clearing and settlement volume.

184. However, even the large international banks worried about attracting attention from U.S. authorities when their illegal dollar clearing activities for Iran markedly increased.

185. For example, as detailed below, in 2003, Defendant Commerzbank's employees expressed concern that Commerzbank's increased volume of illegal Eurodollar clearing activities on behalf of Bank Melli and Bank Saderat would draw unwanted attention.

186. In the spring of 2006, the Manhattan District Attorney's Office first discovered evidence of the Conspiracy engaged in by certain European banks (including the Western Bank Defendants herein) on behalf of Iran and Iranian banks.

187. As the New York State Department of Financial Services ("DFS") later observed:

> By 2008 it was clear that this system of wire transfer checks had been abused, and that U.S. foreign policy and national security could be compromised by permitting U-Turns to continue. In November 2008, the U.S. Treasury Department revoked authorization for "U-Turn" transactions because it suspected Iran of using its banks – including the CBI/Markazi, Bank Saderat and Bank Melli – to finance its nuclear weapons and missile programs. *The U.S. also suspected that Iran was using its banks to finance terrorist groups, including Hezbollah, Hamas and the Palestinian Islamic Jihad, and engaging in deceptive conduct to hide its involvement in various other prohibited transactions, such as assisting OFAC-sanctioned weapons dealers*. [Emphasis added].

188. These findings led to a wide-ranging investigation that ultimately resulted in the entry of a series of Deferred Prosecution Agreements ("DPAs") with the Western Bank Defendants

(as well as other European and Japanese banks), and it exposed catastrophic vulnerabilities in America's counter-financing of terrorism ("CFT") security architecture inherent in the U-Turn exemption because foreign banks, including the Western Bank Defendants herein, were actively conspiring with Iran to help it evade U.S. economic sanctions and secret hundreds of billions of dollars through the U.S. financial system undetected.

189. On October 11, 2007, the Financial Action Task Force ("FATF") released a statement of concern that "Iran's lack of a comprehensive anti-money laundering/counter-terrorist finance regime represents a significant vulnerability within the international financial system."

190. FATF's statement further noted that "FATF members are advising their financial institutions to take the risk arising from the deficiencies in Iran's AML/CFT regime into account for enhanced due diligence."

191. The U.S. criminal investigations would ultimately find that "the risk arising from the deficiencies in Iran's AML/CFT regime" ultimately included willful money laundering and terror financing by Iran with the *active*, ***critical*** assistance of the Defendants herein.

192. Based on figures from both the International Monetary Fund and the Central Bank of Iran, from 2004 through 2011 Iran's total revenues from oil and natural gas export sales totaled approximately $972.9 billion USD.

193. Without the Conspiracy between the Defendants herein, and other foreign financial institutions, Iran could not have (a) transferred the overall volume of USD funds through the international financial system that it did; (b) surreptitiously transferred large amounts of these USD funds for the benefit of Hezbollah and the IRGC; and (c) exploited the Iranian U-Turn exemption to blind U.S. regulators and law enforcement to the degree, and for the duration, that it did.

194. As former Manhattan District Attorney Robert M. Morgenthau pointedly told Congress in 2009, "the U-Turn exemption constituted a glaring hole that undermined both the enforcement of, and the rationale behind, the Iranian sanctions program."

195. Effective November 10, 2008, OFAC revoked the U-Turn exemption in its entirety, and, as of that date, U.S. depository institutions were no longer authorized to process any Iranian U-Turn payments.

196. In announcing the revocation of the U-Turn exemption on November 6, 2008, Treasury stated:

> The U.S. Department of the Treasury today announced that it is revoking the "U-turn" license for Iran, further restricting Iran's access to the U.S. financial system. **Treasury's move today follows a series of U.S. government actions to expose Iranian banks' involvement in the Iranian regime's support to terrorist groups** and nuclear and missile proliferation. (Emphasis added).

197. As part of that announcement, Treasury further explained:

> Iran's access to the international financial system enables the Iranian regime to facilitate its support for terrorism and proliferation. The Iranian regime disguises its involvement in these illicit activities through the use of a wide array of deceptive techniques, specifically designed to avoid suspicion and evade detection by responsible financial institutions and companies. Iran also is finding ways to adapt to existing sanctions, including by turning to non-designated Iranian banks to handle illicit transactions.
>
> The Treasury Department is taking a range of measures, including today's action, to counter these deceptive activities.

198. From that date forward, every financial institution was on formal notice that Iran and Iranian banks had exploited the U-turn" license to provide "support to terrorist groups."

F. LETTERS OF CREDIT – AN ALTERNATIVE METHOD OF UNDERMINING THE IRANIAN SANCTIONS PROGRAM

1. Terminology

199. Letters of Credit ("LCs") are often used in international transactions to ensure that

payment will be received. Due to the nature of international transactions, including factors such as the distance goods must travel, differing laws in each country, and the difficulty of trading parties knowing each party personally, the use of LCs has become a very important aspect of international trade.

200. The LC transaction process begins when an "Applicant" opens the Letter of Credit with a bank.

201. Normally, the Applicant is the purchaser of goods and the LC is opened with his/her bank according to the terms and conditions of the purchase order and business contract between buyer and seller.

202. The "Beneficiary" of the LC is the party to the transaction who receives the payment amount agreed upon in the LC.

203. In order to receive payment for the goods, the Beneficiary company submits all required documents under the terms and conditions of the LC.

204. When an LC is required to be secured, an "Issuing Bank" agrees to guarantee payment for its customer upon the completion of the terms and conditions of the LC.

205. The Issuing Bank's role is to provide a guarantee to the seller that if the required documentation is presented, the bank will examine the documents and pay the contract sum if these documents comply with the terms and conditions set out in the LC.

206. Typically, the documents requested will include a commercial invoice, a transport document such as a bill of lading or airway bill and an insurance document; there are many other documents such as certificates of origin, packing lists and inspection certificates that can be included. LC transactions deal in documents, not in the underlying goods themselves.

207. An "Advising Bank" is usually a foreign correspondent bank of the Issuing Bank that will advise the beneficiary of the transaction. Generally, a Beneficiary of an LC wants to use a local bank to ensure that the LC is valid.

208. In addition, the Advising Bank is usually responsible for sending the documentation to the Issuing Bank. Generally, the Advising Bank has no other obligation under the LC. If the Issuing Bank does not pay the beneficiary, the Advising Bank is not obligated to pay the obligation under the LC.

209. The "Confirming Bank" is usually a correspondent bank that confirms the LC for the Beneficiary. At the request of the Issuing Bank, the Confirming Bank obligates itself to ensure payment under the LC.

210. Because the Confirming Bank does not confirm the credit until it evaluates the country and bank where the LC originates, the Confirming Bank usually acts as the Advising Bank.

211. In the middle of this serpentine process is the "Negotiating Bank," which negotiates documents delivered by the Beneficiary of the LC.

212. The Negotiating Bank examines the drafts and/or documents and verifies and confirms the terms and conditions under the LC on behalf of the Beneficiary to avoid discrepancies.

213. A Negotiating Bank gives value to, and relies upon (or may rely upon), such drafts and/or documents, and may purchase or agree to purchase the drafts and/or documents presented.

214. A Reimbursing Bank usually pays part or all of the amount due to the Beneficiary of the LC on behalf of the Issuing Bank once it receives a statement from the Negotiating Bank that the documents required comply with the LC's terms; however, in certain cases a Reimbursing Bank serves only as a guarantor for the payment by the Issuing Bank.

2. The U.S. Trade Embargo – United States Munitions List (USML) and Commerce Control List (CCL)

215. For decades, U.S. trade with Iran has been carefully circumscribed by the International Traffic in Arms Regulations ("ITARs"), Export Administration Regulations ("EARs"), and Iran Trade Regulations ("ITRs").

216. Certain types of U.S. defense articles and defense services, such as nuclear or conventional weapon systems, are identified based on the ITARs promulgated by the U.S. Department of State and its Directorate of Defense Trade Controls through a publically available United States Munitions List ("USML").[18]

217. In addition to USML items, certain types of U.S. dual-use products, such as nuclear materials, aerospace and other potentially sensitive materials, are identified based on the EARs and ITRs by the U.S. Department of Commerce and its Bureau of Industry and Security ("BIS") on a publicly available Commerce Control List ("CCL").[19]

218. Dual-use items that are not published on the CCL by BIS are commonly referred to by U.S. manufacturers and shipping companies as "EAR99."

219. These EAR99 items generally consist of low-technology consumer goods and do not always require a license; however, shipment from the United States of an EAR99 item to Iran, or any other embargoed country, often requires disclosure to BIS in addition to a license from the Commerce Department.

---

[18] The updated USML is available at: https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf.

[19] The updated list is available at http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

220. As set forth below, one of the aims of the Conspiracy was to evade the U.S. ITARs, ITRs, and EARs—and also various EU decisions and U.N. Security Council Resolutions—prohibiting Iran from conducting both conventional weapons-trafficking and WMD proliferation.

221. To facilitate this aim, Iran and its Co-Conspirators, including the Defendants herein, used LCs drawn on the CBI and other Iranian banks (and "stripped" the underlying payment orders), to clandestinely obtain and transport goods, technologies and weapons that were listed on the USML and/or CCL.

222. Because the IRGC and Hezbollah needed to transport their terrorist operatives and weapons into Iraq, U.S. export-controlled item acquisitions financed by Letters of Credit were instrumental in facilitating the activities of these terrorist organizations, including, but not limited to, helping Iran acquire component parts and technologies used to make the IEDs, EFPs, and Improvised Rocket-Assisted Munitions ("IRAMs") that were deployed by the Iraqi Special Groups against Coalition Forces.

G. IRAN'S ILLEGAL ARMS SHIPMENTS THROUGH ISLAMIC REPUBLIC OF IRAN SHIPPING LINES (IRISL)

223. As Iran's national maritime carrier, IRISL has a long history of facilitating arms shipments on behalf of the IRGC and the Iranian military, including copper discs that are a key component in EFPs (discussed below) used to kill and maim U.S. service members.[20]

224. For example, a November 2007 State Department cable noted:

> Washington remains concerned about on-going conventional arms transfers from China to Iran, particularly given Iran's clear policy of providing arms and other support to Iraqi insurgents and terrorist groups like the Taliban and Hezbollah….

[20] IED is a term commonly used by the U.S. military as shorthand for a roadside bomb. However, unlike IEDs, the EFPs deployed by the IRGC, Hezbollah and the Special Groups in Iraq were not "improvised." Instead, these advanced weapons were professionally manufactured and specifically designed to defeat the armor plating that protected the vehicles used by U.S. and Coalition Forces.

> We have specific information that Chinese weapons and components for weapons transferred to Iran are being used against U.S. and Coalition Forces in Iraq, which is a grave U.S. concern.

225. The diplomatic cable went on to note that an IRISL-flagged vessel was loaded at a Chinese port with multiple containers of cargo bound for delivery at the port of Bandar Abbas, Iran.

226. The cargo included Iranian Defense Industries Organization ("DIO")[21] manufactured ammunition cartridges (7.62 x 39 rounds for AK-47 assault rifles).

227. DIO is an Iranian government-owned weapons manufacturer controlled by MODAFL.

228. An April 2008 State Department cable warned of an IRISL shipment of chemical weapons precursors from China aboard the IRISL-leased, Iranian flagged merchant vessel ("M/V") *Iran Teyfouri*.

229. In September 2008, the U.S. Treasury Department designated IRISL an SDN, stating: "Not only does IRISL facilitate the transport of cargo for U.N. designated proliferators, it also falsifies documents and uses deceptive schemes to shroud its involvement in illicit commerce."

230. The Treasury Department further noted that:

> [i]n order to ensure the successful delivery of military-related goods, IRISL has deliberately misled maritime authorities through the use of deception techniques. These techniques were adopted to conceal the true nature of shipments ultimately destined for MODAFL [Iran's Ministry of Defense and Armed Forces Logistics].

[21] DIO was designated an SDN by the U.S. on March 30, 2007. IRGC Brigadier-General Seyyed Mahdi Farahi was the Managing Director of DIO and has been sanctioned by the EU since 2008 (*see,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0475). He was later sanctioned by the U.S. on January 17, 2016.

231. In January 2009, a former Russian merchant ship chartered by IRISL—named the M/V *Monchegorsk* and flying a Cypriot flag—was spotted leaving the Iranian port of Bandar Abbas and heading for the Suez Canal.

232. Egyptian authorities were alerted by the U.S. Navy, and the M/V *Monchegorsk* was forced into an Egyptian port to be searched. Iran's DIO was later determined to be the shipper of the military-related cargo.

233. Munitions, believed headed for Gaza, were found hidden in the cargo, including components for mortars and thousands of cases of powder, propellant, and shell casings for 125mm and 130mm guns.

234. In October 2009, U.S. troops boarded a German-owned freighter, the M/V *Hansa India*, in the Gulf of Suez and found eight containers full of ammunition that were headed to Syria from Iran.

235. The vessel carried seven containers of small arms ammunition (including 12 million bullet casings), as well as one container containing copper discs of the type used in EFPs to kill and maim hundreds of U.S. service members.

236. The acronym "IRISL" was painted in large block letters on the exterior side walls of each shipping container, and the barrels of munition parts discovered inside the containers were marked with the inscription "SAEZMANE SANAYE DEFA," a common transliteration from Farsi to English of the name for Iran's Defense Industries Organization (DIO).

237. The M/V *Hansa India* was registered to the Hamburg-based shipping company Leonhardt & Blumberg but had been under charter to IRISL for several years.

238. In November 2009, the Government of Israel intercepted an IRISL-flagged ship, the M/V *Francop*, headed for Beirut, Lebanon and then Latakia, Syria. The vessel was loaded with

munitions crates that were either stamped "IRISL" or included documentation marked with the IRGC-QF logo.

239. The munitions found onboard included over two thousand 107mm "Katyusha" rockets, more than six hundred 122mm "Grad 20" rockets, and also various rocket fuses, mortar shells, rifle cartridges, fragment grenades and 7.62mm bullets.

240. The M/V *Francop*, owned by the Cypriot shipping company UFS, was carrying shipping containers clearly marked IRISL.

241. United Nations Security Council Resolution 1929, adopted on June 9, 2010, froze certain assets of IRISL and called on the international community to cease providing financial and insurance services to both the IRGC and IRISL.

242. In addition, a July 2010 European Union ("EU") sanctions implementing regulation confirmed that IRISL conducted deceptive business practices in order to access USD funds.

243. Specifically, EU Council Implementation Regulation Number 668/2010 stated that "IRISL subsidiaries have used US dollar-denominated bank accounts registered under cover-names in Europe and the Middle East to facilitate routine fund transfers."

244. Similarly, the June 2011 indictment of IRISL in New York stated:

> In many aspects of global commerce, including the international maritime industry, contracts and payments are denominated in U.S. dollars. Such U.S. dollar transactions are primarily executed, or "cleared," through correspondent banks in the United States. The U.S. dollar clearing operations for many large U.S. financial institutions are processed through correspondent bank accounts domiciled in New York County.
>
> In order to deceive and bypass these OFAC filters, SDNs designated under OFAC's non-proliferation of weapons of mass destruction program must falsify, or cause to be falsified, the originator and/or beneficiary information in wire transfers. In other words, by omitting or falsifying data regarding their roles as the true originators or beneficiaries, SDNs are able to send and receive wire transfers that would otherwise be blocked by U.S. financial institutions. Through the fraudulent use of a web of subsidiary entities and

front companies, IRISL and the other defendants were able to deceive U.S. financial institutions and maintain their access to the U.S. financial system.

245. Because the DIO, as discussed *infra*, was one of MODAFL's three main weapons systems manufacturers, it was required to use IRISL for most of its illicit shipments of military-related raw-materials, parts and finished products for, and from, foreign suppliers, Iranian arms dealers and terrorist organizations.

246. Iran's DIO was listed as an entity of concern for military procurement activities in an early warning document distributed by the German government to industry in July 2005.

247. The DIO was also designated by the United Nations in 2006 for its involvement in Iran's WMD program.

248. During 2006 and 2007, weapons caches seized by Coalition Forces from the Special Groups in Iraq contained large quantities of weapons produced by Iran; including many 107 millimeter artillery rockets with closely clustered DIO lot numbers and production dates between 2005 and 2007, as well as rounds and fuses for 60 millimeter and 81 millimeter mortars with DIO lot markings and 2006 production dates.

249. In sum, at no point in time was the DIO a legitimate agency of the Iranian government.

250. According to the U.S. State Department, the DIO was the owner of a Eurodollar account that was maintained by Bank Melli Iran's branch in Hamburg; and this bank account was used to send and receive USD funds transfer transactions for the benefit of the DIO.

251. Bank Melli Iran's branch in Hamburg was a customer of Defendant Commerzbank during the relevant period, and both Bank Melli Iran and Commerzbank were active participants in the Conspiracy set forth herein.

H. THE IRGC AND HEZBOLLAH COMMITTED ACTS OF INTERNATIONAL TERRORISM AT IRAN'S DIRECTION IN WHICH PLAINTIFFS WERE FORESEEABLY INJURED

252. As previously noted, Iran has had a long, deep, strategic partnership with the Lebanese-based Foreign Terrorist Organization Hezbollah, which historically has served as Iran's proxy and agent, enabling Iran to project extremist violence and terror throughout the Middle East and around the globe.

253. After the U.S. and its Coalition partners invaded Iraq in March 2003, Iran embarked on a calculated and carefully calibrated campaign in Iraq.

254. Iran's multifaceted goals included killing and maiming U.S. service members and other Coalition Forces (primarily Polish and British personnel), as well as Iraqi civilians, in Iraq in order to induce Coalition Forces to leave Iraq; expanding Iranian influence in Iraq; and promoting an Iraqi government subservient to Iran.

255. Iran was unable to confront the U.S. with its conventional military, or to risk provoking a U.S. military response, so it decided to employ its preferred method of statecraft: a terror campaign.

256. Iran's two primary instruments for conducting this terrorist campaign against Coalition Forces were Lebanese Hezbollah (designated a Foreign Terrorist Organization by the United States in 1997) and the IRGC (designated an SDGT by the United States in 2017 and an FTO in 2019) including its foreign operations and terrorism directorate, the IRGC-QF (designated an SDGT by the United States in 2007 and an FTO in 2019).

257. The United States designated the IRGC-QF an SDGT for, *inter alia*, "provid[ing] lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi'a militants who target and kill Coalition and Iraqi forces and innocent Iraqi civilians."

258. In 2017, Congress found that the IRGC-QF "is the primary arm of the Government of Iran for executing its policy of supporting terrorist and insurgent groups. The IRGC-QF provides material, logistical assistance, training, and financial support to militants and terrorist operatives throughout the Middle East…."

259. As noted above, on April 15, 2019, the United States designated the IRGC an FTO, noting that:

> The Iranian regime is responsible for the deaths of at least 603 American service members in Iraq since 2003. This accounts for 17% of all deaths of U.S. personnel in Iraq from 2003 to 2011, and is in addition to the many thousands of Iraqis killed by the IRGC's proxies.[22]

260. While the IRGC and the IRGC-QF were responsible for managing Iran's terror campaigns abroad, they lacked recent operational and tactical experience in developing terrorist capabilities and performing terrorist attacks against a modern military force. Moreover, as ethnically Persian, Farsi-speaking entities, IRGC personnel were at a disadvantage in recruiting and training ethnically Arab, Arabic-speaking Shi'a Iraqis.

261. For that purpose, the IRGC-QF therefore turned to FTO Hezbollah, Iran's Lebanese long-standing terror proxy, which had hard-earned experience in running terror campaigns against the Israel Defense Forces in Lebanon, and which shared ethnic and language connections with Iraqis.

262. Hezbollah and the IRGC-QF worked symbiotically to plan, authorize, and commit attacks on Coalition Forces in Iraq. They accomplished this by developing agents among the Shi'a population in Iraq, providing them with funding, weapons, and training, and then guiding and directing them to attack Coalition Forces.

---

[22] https://www.state.gov/designation-of-the-islamic-revolutionary-guard-corps/

263. Specifically, the IRGC-QF and Hezbollah provided these proxies with sophisticated weapons specially designed to inflict casualties on the well-protected Coalition Forces—principally, EFPs and IRAMs, along with the Tactics, Techniques, and Procedures ("TTPs") developed by Hezbollah necessary to use them most effectively.

264. These Shi'a proxies included:

- **Badr Corps/Badr Organization**,
- **Jaysh al-Mahdi** ("JAM" or the "Mahdi Army") including the Promised Day Brigades
- **Asa'ib Ahl Al-Haq** ("AAH" or the "League of the Righteous")
- **Kata'ib Hezbollah** (KH) (designated an FTO in 2009).

265. Although the precise roles and proficiencies of these groups evolved over time, at all relevant times each acted as the agent of Hezbollah and the IRGC-QF in attacking Coalition Forces.

266. The IRGC-QF provided EFPs to their proxies for the *exclusive* purpose of targeting Coalition Forces, and Hezbollah's advanced EFP training was provided exclusively to these cells to improve their emplacement of EFPs against Coalition armored vehicles. The IRGC-QF and Hezbollah were the sole sources of the weapons.[23]

267. These terror cells served as EFP emplacers (or in some cases, trigger pullers) for the IRGC-QF and Hezbollah. They were generally not permitted to use their independent judgment in choosing their targets (they were often directed to select a particular date or location for an attack, and even required to provide visual evidence that they had carried out the IRGC's directives). If a group or cell failed to comply with the IRGC's directives it could be deprived of EFPs and other support. EFPs were carefully controlled. For example, "[e]ach major arms cache

[23] In 2007, when AAH founder Qais Khazali was captured by Coalition Forces, he acknowledged that "EFPs still come solely from Iran and there is currently nobody in Iraq manufacturing the components of an EFP."

[had] a 'hide custodian' who signs out weapons such as EFPs and is responsible for their proper use against U.S. forces and the minimization of Iraqi casualties."[24]

268. When EFPs were misused, the IRGC cut the group off.[25]

269. A 2010 Department of Defense report confirmed that weapons Iran delivered to Shi'a groups in Iraq included EFPs (with radio-controlled, remote arming and passive infrared detonators), IEDs, anti-aircraft weapons, mortars, 107 and 122mm rockets, rocket-propelled grenades and launchers, explosives, and small arms.

270. In the post-invasion period, the lethality of Shi'a attacks on U.S. and Coalition Forces was the direct result of the IRGC's policy. And the terrorist cells that in fact targeted U.S. service members were created and sustained by the IRGC and Hezbollah for that purpose.

1. The IRGC

271. The IRGC is a paramilitary force answerable only to the Supreme Leader of Iran himself. The IRGC's devotion to Ayatollah Khamenei is "a religious imperative," because the IRGC is the Supreme Leader's personal force. The IRGC differs from Iran's "regular" armed forces, which ostensibly functions under a national command structure. The IRGC is tasked with "protecting the revolution," which it accomplishes by silencing perceived enemies at home through secret police methods and attacking perceived enemies abroad (via its Qods Force) through terrorist tactics. It also aids in Iran's development of weapons of mass destruction, including EFPs and IRAMs and its nuclear program.

272. As the U.S. Treasury Department explained in designating the IRGC an SDGT,

---

[24] *See* Michael Knights, The Evolution of Iran's Special Groups in Iraq, CTC Sentinel, U.S. Military Academy at West Point (Nov. 2010), *available at* https://ctc.usma.edu/app/uploads/2011/05/CTCSentinel-Vol3Iss11-127.pdf.

[25] On rare occasions, certain elements defied this directive. For example, EFPs were used in the assassinations of two provincial governors and two provincial police chiefs in the latter half of 2006. The U.S. military assessed that these events were contrary to IRGC policy.

"[t]he IRGC has played a central role to Iran becoming the world's foremost state sponsor of terror." Treasury also designated the IRGC "for the activities it undertakes to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of" its foreign operations directorate, the IRGC-QF.

273. Also, in 2017, Congress found that "the IRGC, not just the IRGC-QF, is responsible for implementing Iran's international program of destabilizing activities, support for acts of international terrorism, and ballistic missile program."

274. As the U.S. Treasury Department explained in designating the IRGC for a third time, it was also "previously designated pursuant to E.O. 13382 on October 25, 2007, in connection with its support to Iran's ballistic missile and nuclear programs, and pursuant to E.O. 13553 on June 9, 2011 and E.O. 13606 on April 23, 2012, in connection with Iran's human rights abuses."

275. As noted above, the IRGC was designated an FTO on April 15, 2019 in part for its role in the deaths of at least 603 American service members in Iraq since 2003.

276. To fund and supply its terror apparatus, the IRGC owns or controls a significant number of Iran's private and public companies. According to a 2007 *Los Angeles Times* report, the IRGC has ties to over 100 companies, controlling billions of dollars in assets. These funds fuel the IRGC's terrorist operations, secret policing, and WMD efforts.

277. As a Council on Foreign Relations assessment has noted, the IRGC is:

> [H]eavily involved in everything from pharmaceuticals to telecommunications and pipelines – even the new Imam Khomeini Airport and a great deal of smuggling. Many of the front companies engaged in procuring nuclear technology are owned and run by the Revolutionary Guards. . . . It's a huge business conglomeration.

278. The U.S. has designated these businesses or identified them as IRGC agents whenever possible. For example, 143 entities and individuals are currently sanctioned as operating

under IRGC control (more were sanctioned during the relevant period, but some sanctions were removed as a result of negotiations related to the Joint Comprehensive Plan of Action, also known as the "JCPOA" or "Iran Nuclear Deal").These include Khatam al-Anbia, which, according to the U.S. Treasury Department, is "a construction and development wing of the IRGC that generates income and *funds operations for the IRGC*."

279. It also includes NIOC, which the U.S. Treasury Department found was "an agent or affiliate of the" IRGC. As a result, the U.S. Treasury Department blocked NIOC's property pursuant to the International Emergency Economic Powers Act. "This means that foreign financial institutions determined to knowingly facilitate significant transactions or provide significant financial services for NIOC will be subject to [Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010] sanctions, including the prohibition or the imposition of strict conditions on the opening or maintaining of correspondent or payable-through accounts in the United States." In reporting that finding, Treasury emphasized the IRGC's "support for terrorism" and "history of attempting to circumvent sanctions by maintaining a complex network of *front companies*." (Emphasis added.)

280. In fact, the U.S. Treasury Department has recently noted that "[t]he international community must vehemently reject Iranian oil and related products in the same way that it rejects the violent acts of terrorism these [oil-for-terror] networks fund."[26]

281. These businesses are crucial to the IRGC's terror apparatus. The IRGC pays salaries of vast numbers of personnel both in Iran and abroad (including in Iraq) and funds training centers

[26] Press Release, U.S. Dep't of the Treasury, "Treasury Designates Vast Iranian Petroleum Shipping Network That Supports IRGC-QF and Terror Proxies," (Sept. 4, 2019) *available at* https://home.treasury.gov/news/press-releases/sm767.

and schools for up-and-coming terrorists. It also funds an enormous weapons production system, from ballistic missiles to EFPs.

282. In designating the IRGC's Basij militia (Basij is one of the IRGC's armed force components), the U.S. Treasury Department explained that IRGC and other elements of the Iranian military "have expanded their economic involvement in major industries and infiltrated seemingly legitimate businesses to fund terrorism and other malign activities. This vast network provides a financial lifeline to the Basij's efforts to recruit, train, and indoctrinate child soldiers as young as twelve who are coerced into combat under the IRGC's direction."

283. In short, the IRGC funds its primary operations—terrorism, domestic repression and WMD development—through corporations under its control.

2. The IRGC-QF

284. In July 2007, MNF-I spokesman General Kevin J. Bergner briefed the media on how the IRGC-QF employed Hezbollah operatives in Iraq: "Iran's Quds Force, a special branch of Iran's Revolutionary Guards, is training, funding and arming the Iraqi groups…. Iranian operatives are using Lebanese surrogates to create Hezbollah-like capabilities. And it paints a picture of the level of effort in funding and arming extremist groups in Iraq."

285. In October 2007, the U.S. Treasury Department designated the IRGC-QF as an SDGT, finding:

> The Qods Force has had a long history of supporting Hizballah's military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support. The Qods Force operates training camps for Hizballah in Lebanon's Bekaa Valley and has reportedly trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran. The Qods Force provides roughly $100 to $200 million in funding a year to Hizballah and has assisted Hizballah in rearming in violation of UN Security Council Resolution 1701.

> In addition, the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi'a militants who target and kill Coalition and Iraqi forces and innocent Iraqi civilians.

286. The U.S. State Department's Country Reports on Terrorism for 2007 stated:

> The [IRGC-QF] continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, mortars that have killed thousands of Coalition and Iraqi Forces, and explosively formed projectiles (EFPs) that have a higher lethality rate than other types of improvised explosive devised (IEDs) and are specially designed to defeat armored vehicles used by Coalition Forces. The Qods Force, in concert with Lebanese Hezbollah, provided training outside Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry.

287. The U.S. State Department's Country Reports on Terrorism for 2008 reported that Iran was:

> Provid[ing] lethal support, including weapons, training, funding, and guidance, to Iraqi militant groups that targeted Coalition and Iraqi forces and killed innocent Iraqi civilians. Iran's Qods Force continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, and mortars that have killed Iraqi and Coalition Forces as well as civilians. Tehran was […] providing militants with the capability to assemble improvised explosive devices (IEDs) with explosively formed projectiles (EFPs) that were specially designed to defeat armored vehicles. The Qods Force, **in concert with Lebanese Hezbollah**, provided training both inside and outside of Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry. (Emphasis added.)

288. On January 9, 2008, the U.S. Department of the Treasury designated Ahmed Foruzandeh, a Brigadier General in the IRGC-QF, finding:

> As of mid-February 2007, Foruzandeh ordered his Iranian intelligence officers to continue targeting Shia and Sunnis to further sectarian violence within Iraq. Foruzandeh is also responsible for planning training courses in Iran for Iraqi militias, including Sayyid al-Shuhada and Iraqi Hizballah [KH], to increase their ability to combat Coalition Forces. The training includes courses in guerilla warfare, light arms, marksmanship, planting improvised explosive devices (IEDs), and firing anti-aircraft missiles.

289. At a July 2, 2007 press briefing, General Bergner noted:

> The Qods Force also supplies the special groups with weapons and funding of 750,000 to 3 million U.S. dollars a month. Without this support, these special groups would be hard pressed to conduct their operations in Iraq […] The Qods Force goal was to develop the Iraqi special groups into a network similar to the Lebanese Hezbollah. Special groups would be unable to conduct their terrorist attacks in Iraq without Iranian-supplied weapons and other support.

3. Lebanese Hezbollah and Unit 3800

290. As noted above, the relationship between the Iranian regime and Hezbollah is, and has been since the latter's creation, symbiotic.

291. The early Lebanese Shi'a clerics who emerged from the seminaries in Najaf (Iraq) and Qom (Iran) included Musa al-Sadr and Ayatollah Muhammad Hussein Fadlallah (Hezbollah's spiritual leader).

292. Like the late Ayatollah Muhammad Sadiq al-Sadr in Iraq, Musa al-Sadr is credited with first mobilizing the previously passive and marginalized Shi'a community in Lebanon by inspiring the foundation of the Amal movement which eventually gave birth to Hezbollah.

293. Musa al-Sadr disappeared (and was likely murdered) in Libya in 1978 which created an opening for Sadr's contemporary, Muhammad Hussein Fadlallah, to whom much of Musa al-Sadr's influence and power passed.

294. In June 1982, Sayyid Hussein al-Musawi, a member of Amal's command council, broke with the movement and founded "Islamic Amal," which soon transformed into Hezbollah.

295. Hezbollah's founders also included Subhi al-Tufayli, Muhammad Yazbek, Na'im Qasim, Ibrahim Amin al-Sayyid, and Hassan Nasrallah (who would later emerge as Hezbollah's leader).

296. Inspired by the success of Iran's Islamic revolution and influenced by Ayatollah Khomeini's ideological worldview, these young fanatics set to work building a network in Lebanon that was directly answerable to the Iranian Supreme Leader.

297. Since the early 1980s, Iran's IRGC has helped Hezbollah equip itself not only with vast supplies of weapons and explosive devices but also with broadcasting, healthcare, and educational centers to expand its political and social reach within Lebanon. For example, Iran spends millions of dollars in Lebanon on the construction of bridges, roads, schools, and hospitals.

298. To this day, Ayatollah Ali Khamenei, the current supreme leader of the Islamic Republic, maintains various offices in the southern suburbs of Beirut and in southern Lebanon. These offices serve as the official religious headquarters of the Ayatollah, but the Iranian intelligence service and Hezbollah also use these facilities for information gathering, political and security meetings, and surveillance, and as military courts for their prisoners.

299. The Iranian government hosts hundreds of Hezbollah-affiliated Lebanese students each year in Iranian universities and seminaries, especially in Qom.

300. The Iranian-funded welfare programs for Lebanese Shi'a are backed by a very professional and energetic propaganda machine that not only extols Hezbollah and its Iranian patron but also seeks to elevate Khamenei, who competes with the Grand Ayatollah Ali Hussein al-Sistani (based in Iraq) who espouses a less overtly political form of Shi'ism.

301. Iranian clerics, especially Ayatollah Khamenei (with the help of the IRGC) pay monthly salaries to the roughly 2,500 Shi'a clerics of Lebanon, further cementing their loyalty to the Iranian regime.

302. When Hezbollah leader Hassan Nasrallah met with Iran's supreme leader Ayatollah Khamenei in 2001, Nasrallah publicly kissed Khamenei's hand, a gesture heavy with meaning among the Shi'a: it implied that Nasrallah accepts Khamenei as his leader.

303. Yet, when the U.S. entered Iraq in 2003, there was no immediate expectation that Hezbollah would follow.

304. One of the first indications that Hezbollah operatives might be present in Iraq after the U.S.-led invasion came in an article in *The New York Times* published in November 2003 that stated:

> Both American and Israeli intelligence have found evidence that Hezbollah operatives have established themselves in Iraq, according to current and former United States officials. Separately, Arabs in Lebanon and elsewhere who are familiar with the organization say Hezbollah has sent what they describe as a security team of up to 90 members to Iraq. The organization has steered clear of attacks on Americans, the American officials and Arabs familiar with Hezbollah agree.

305. In retrospect, another early warning sign occurred in May 2003 when Israeli naval commandos seized a small fishing boat off the country's northern coast and captured a Hezbollah explosives expert who had bomb detonators and computer disks on board.

306. The computer disks contained instructions on how to manufacture and assemble EFPs, providing granular details on the key elements required to make them effective against armored vehicles, including the specifications for the concave copper liners needed for maximum lethality.

307. Sometime in 2003, the IRGC-QF instructed Hezbollah to create "Unit 3800," an entity dedicated to developing and supporting Iraqi Shi'a terrorist cells which would execute IRGC and Hezbollah attacks on Multi National Forces in Iraq ("MNF-I").

308. Unit 3800 was established by Hezbollah leader Hassan Nasrallah at Iran's behest.

309. Unit 3800 later trained, advised and directed the JAM "Special Groups" and Badr Corps in Iraq.

310. Hezbollah's expertise in the use of EFPs and other weapons, kidnapping, communications and small-unit operations were critical to the effectiveness of the IRGC's proxies in Iraq between 2004 and 2011.

311. As former Badr Corps leader and KH founder Abu Mahdi al-Muhandis (discussed below) would later explain to the Hezbollah-affiliated channel *Al-Mayadeen*:

> **Muhandis:** Of course, my relationship with martyr Imad, the great martyr Imad [Mughniyah], and martyr Mustafa Badr a-Din, started in the early 1980s. This was a strong and operational relationship. The first ones to train the first Iraqi jihadi resistance groups in the beginning of the 1980s were Imad and Mustafa. They also had a major role in organizing the resistance cells against the Americans in Iraq.
>
> **Host:** Training Iraqis here, to fight the Americans?
>
> **Muhandis:** Sure, they trained Iraqis. The first Iraqi cells, I was among them, after 2003.
>
> **Host:** After 2003…
>
> **Muhandis:** They had a major role, their brothers and men still have an essential role in training and planning… they have a very important role.

312. A 2010 Department of Defense report noted that "Lebanese Hizballah provides insurgents with the training, tactics and technology to conduct kidnappings, small unit tactical operations and employ sophisticated IEDs."

313. A July 2004 UK Joint Intelligence Committee ("JIC") assessment noted: "We also judge that Lebanese Hizballah will retain an influence in Iraq (Hizballah members may have been linked to the group that attacked the Sheraton Hotel) and could supply Iraqi groups with terrorist expertise and munitions."

314. Tracing Hezbollah's carefully monitored introduction of EFPs, the UK Defence Intelligence Staff ("DIS") accurately predicted on August 3, 2004, the evolution of the IED threat in Iraq: "IED technology in use with other Middle Eastern groups[,] especially Lebanese Hizballah, can be expected to appear in Iraq. This would include multiple systems, such as RC (Radio-Controlled) switched PIRs [Passive Infrared]."

315. By the summer of 2004, British intelligence had detected the EFP's appearance in southern Iraq:

> On 26 July, the DIS reported that an EFP IED had been found on 15 July in Baghdad. The DIS noted that the EFP IED design had not previously been encountered in Iraq but was, as with the find in May 2004, of a type associated with Lebanese Hizballah. There were also indications of Iranian involvement in the construction of the devices.

316. On December 2, 2004, a British Defence Intelligence Report titled "The Evolution of the IED Threat in Iraq" stated:

> Improvement in IED technology has been most significant in Shia areas since May [20]04, where technical progress has been made that we assess could only have been achieved through focused external assistance. **We assess that this may be due to an influx of Lebanese Hezbollah IED technology under Iranian sponsorship."** (Emphasis added.)

317. Similarly, the United States Department of State Country Reports on Terrorism 2006 reported:

> Since at least 2004, Hizballah has provided training and logistics to select Iraqi Shia militants, including for the construction and use of shaped charge IEDs, which Hizballah developed against Israeli forces in southern Lebanon during the late 1990s and which can penetrate heavily armored vehicles.

318. The Australian government reported in 2006:

> Hizballah has established an insurgent capability in Iraq, engaging in assassinations, kidnappings and bombings. The Hizballah units have been set up with the encouragement and resources of Iran's Revolutionary Guards al Qods Brigades. Hizballah has also established a special training

cell known as Unit 3800 (previously known as Unit 2800) specifically to train Shia fighters prior to action in Iraq.

VI. THE IRGC-QF'S AND HEZBOLLAH'S DEVELOPMENT AND DIRECTION OF SHI'A TERRORIST GROUPS AND CELLS IN IRAQ TO ATTACK COALITION FORCES.

A. THE BADR CORPS/BADR ORGANIZATION

319. The Badr Corps was established in 1982 as the military wing of the Supreme Council for Islamic Revolution in Iraq ("SCIRI"), which was founded by Muhammad Baqr Hakim in the same year. The Badr Corps and SCIRI served as part of the Iranian attempt to influence Shi'a Iraqis during the Iran-Iraq war. The Badr Corps fought Saddam Hussein's forces on Iran's behalf during that war.

320. From its headquarters in Iran, the Badr Corps operated extensive networks throughout Iraq in the 1990s. The group smuggled men and weapons into Iraq to conduct attacks against the Iraqi Ba'athist regime of Saddam Hussein (the Ba'athist regime was dominated by Sunnis and repressed the Shi'a majority population). The Badr Corps had long established four geographic commands inside Iraq, all with experience conducting attacks against the Hussein regime.

321. Like Hezbollah in Lebanon, the Badr Corps established clandestine offices in businesses and social organizations in Iraq. The Badr Corps also used Iraqi front companies to recruit operatives, collect intelligence, and circulate propaganda materials in Shi'a populated areas.

322. Before 2003, the Badr Corps served as Iran's most important surrogate inside Iraq, acting as a *de facto* arm of the IRGC-QF.

323. The Badr Corps continuously received training, weapons and direction from the IRGC and Hezbollah.

324. Following the toppling of the Hussein regime in 2003, the IRGC saw an immediate

opportunity to repatriate Muhammad Baqr Hakim to Iraq and carefully cultivate his party's growth within the new post-war political framework being developed by the Coalition Forces, while simultaneously slipping thousands of Badr Corp fighters back across the border.

325. After 2003, the Badr Corps renamed itself the Badr Organization, and it took on a political component with seats in the new Iraqi parliament through its political wing SCIRI. Nonetheless, despite its sanitized, self-given name, its core essence did not change. It continued playing a significant role in facilitating IRGC-sponsored terror operations in Iraq. Several senior terror cell commanders such as Al-Muhandis are, or were, Badr Corps personnel on the IRGC-QF payroll.

326. The Badr Organization inserted hundreds of its Iranian-trained operatives into Iraq's newly formed state security organs (notably the Iraqi Ministry of Interior intelligence structure and key special forces and Iraqi Army units). This not only assisted in the Badr Organization's efforts to murder former Hussein regime leaders and pursue ethnic cleansing of Sunni neighborhoods, but it also made it possible for the Badr Organization to regularly provide other terror cell operatives with intelligence about Coalition Forces activities and to provide its own terror cells with targeting guidance.

327. Published reports indicate that thousands of members of the Badr Organization remained on the IRGC-QF payroll after 2004.

328. Several senior Badr Organization operatives later emerged as key conduits for funneling Iranian weapons and instructions to Iranian proxies in Iraq from 2004 through 2011, including Abu Mustafa al-Sheibani, a key smuggler of deadly Iranian weapons, including EFPs, and Jamal Ja'far Muhammad, a.k.a. Abu Mahdi al-Muhandis (which is Arabic for "the Engineer"), who later led Special Group KH, which is discussed further below.

329. These Badr Organization operatives also remained (and may still remain) on the IRGC-QF payroll.

330. The IRGC-QF's Ramazan Corps, led by General Abdul Reza Shahlai, was in charge of supporting Hezbollah-trained terror cells in Iraq and remains the largest Qods Force command outside of Iran. It coordinated, armed and directed the Badr Organization.

331. General Shahlai served as the case officer or supervisor of the Special Groups and other proxies, including the Badr Corps cells that acted as such. The United States later designated Shahlai in September 2008 "for threatening the peace and stability of Iraq and the Government of Iraq." The U.S. Treasury Department further found that:

> In late-August 2006, Shahlai provided material support to JAM Special Groups by supplying JAM Special Groups members with 122mm grad rockets, 240mm rockets, 107mm Katyushas, RPG-7s [a predecessor to the RPG-29, the weapon at issue here], 81mms, 60mm mortars, and a large quantity of C-4.
>
> Shahlai also approved and coordinated the training of JAM Special Groups. As of May 2007, Shahlai served as the final approving and coordinating authority for all Iran-based Lebanese Hizballah training for JAM Special Groups to fight Coalition Forces in Iraq. In late-August 2006, Shahlai instructed a senior Lebanese Hizballah official to coordinate anti-aircraft rocket training for JAM Special Groups.

332. The United States Department of State Country Reports on Terrorism 2006 noted:

> Iran provided guidance and training to select Iraqi Shia political groups, and weapons and training to Shia militant groups to enable anti-Coalition attacks. Iranian government forces have been responsible for at least some of the increasing lethality of anti-Coalition attacks by providing Shia militants with the capability to build IEDs with explosively formed projectiles similar to those developed by Iran and Lebanese Hezbollah. The Iranian Revolutionary Guard was linked to armor-piercing explosives that resulted in the deaths of Coalition Forces. The Revolutionary Guard, along with Lebanese Hezbollah, implemented training programs for Iraqi militants in the construction and use of sophisticated IED technology. *These individuals then passed on this training to additional militants in Iraq.* (Emphasis added.)

333. During the first half of 2004, when Hezbollah slowly began to introduce EFPs into Iraq in small numbers at the IRGC's direction, it did so through the Badr Organization.

334. Unlike JAM (discussed below), the Badr Organization had received prior (and extensive) military training from, and its operatives had longstanding operational ties to, Hezbollah and the IRGC.

335. The Baghdad-based command of the Badr Organization was supervised from an IRGC base in nearby Bakhtaran, Iran by Abu Mustafa al-Sheibani, whose extensive smuggling routes were used both before and after the 2003 U.S.-led invasion for transporting weapons, men and money from Iran into Iraq.

336. The most notable Badr Organization cells were the so-called "Sheibani Network" named after him.

337. In January 2009, the U.S. Department of the Treasury designated Abu Mustafa Al-Sheibani for his role as the leader of the Sheibani Network, noting:

> The network's first objective is to fight U.S. forces, attacking convoys and killing soldiers. Its second objective is to eliminate Iraqi politicians opposed to Iran's influence. Elements of the IRGC were also sending funds and weapons to Al-Sheibani's network.
>
> Al-Sheibani's network – consisting of several hundred members – conducted IED attacks against Americans in the Baghdad region. As of March 2007, Al-Sheibani, known to transport Katyusha rockets to be used for attacks against Coalition Forces, launched rockets against Americans and made videos of the attacks to get money from Iran. As of April 2007, a member of Al-Sheibani's network supervised the transport of money and explosives from Iran for eventual arrival in Baghdad. In early-May 2007, Al-Sheibani's network assisted members of a Shia militia group by transporting them to Iran for training and providing them with weapons for their activities in Iraq.

338. According to the Chilcot Report released by the British Government, "[t]he first IED attack in Iraq using an Explosively Formed Projectile (EFP) took place against a UK Warrior

vehicle in al-Amara in May 2004." When Hezbollah introduced the EFP, its most effective anti-armor weapon into Iraq, it began by training Badr Organization operatives.

339. At first, they were trained in the emplacement of single EFPs with relatively primitive initiation systems, a starting point that allowed Hezbollah to test the weapons, assess the capabilities of its Iraqi proxies, and probe Coalition Forces' responses to the threat, attack by attack.

340. By this method of slowly introducing the weapon system and directing its use against British forces, Hezbollah was able to assess the capabilities of the Badr Organization personnel, assess the effectiveness of its own TTPs, and adjust those TTPs based on how first British (and later American) forces responded.

B. JAYSH AL-MAHDI ("JAM" OR THE "MAHDI ARMY")

341. Initially, the Saddam Hussein regime sponsored the late Ayatollah Muhammad Sadiq al-Sadr, a leading Shi'a cleric in Iraq during much of Saddam Hussein's rule. He was perceived to be a relatively moderate counterbalance to the influence of more radical Shi'a religious leaders and was therefore allowed to appoint imams to lead mosques in hundreds of towns and cities.

342. Sadiq al-Sadr used this opportunity to develop a cohesive network under his guidance and control. He was particularly popular in the Shi'a slums of Baghdad and Basra and established a network of mosques and social institutions that attempted to mirror Hezbollah's development in Lebanon.

343. Unlike many of his Shi'a clerical peers, Sadr was not particularly favorably disposed toward Iran, even after the Islamic revolution in 1979, remaining instead an Arab nationalist, and supporting Arab control of the seminaries of Najaf, traditionally dominated by

senior clerics who are either Iranian-born or of Iranian descent.

344. Nonetheless, the Hussein regime ultimately came to regard Sadr as a political threat and assassinated him together with his two oldest sons, leaving his youngest son, Muqtada al-Sadr, as the de facto successor to what became known as the Sadrist Movement.

345. The Sadrist Movement commanded the loyalty of perhaps millions of poor Iraqi Shi'a, but under the Hussein regime's rule it had no military capacity; it was almost exclusively a social and political movement.

346. The 2003 U.S.-led invasion freed Muqtada al-Sadr and his followers from the constraints placed on them by the Hussein regime, and the young Sadr set his sights on becoming the preeminent leader of Iraq's Shi'a community.

347. In June 2003, shortly after the U.S. invasion, Iran's Supreme Leader, Ayatollah Ali Khamenei invited Sadr and his key deputies to Iran in the hope of organizing an armed faction of the Sadrist Movement. IRGC-QF deputy commander Abdul Reza Shahlai therefore served as the "chief of protocol" for the visit and IRGC-QF commander General Qasem Soleimani served as host to the Sadr delegation.

348. Sadr also met with Ayatollah Khamenei during the visit and received assurances from General Shahlai that the IRGC-QF wanted to financially support the Sadrist movement.

349. Shortly thereafter, the IRGC dispatched two of Hezbollah's most senior terror operatives, Imad Mughniyeh and Mustafa Badr al-Din – consecutively leaders of Hezbollah's terror wing known as the Islamic Jihad Organization – to help organize and birth the creation of the Sadrist Movement's armed faction.

350. On July 18, 2003, Sadr gave a sermon in the Great Mosque in Kufa in which he branded the newly-formed Iraqi government "nonbelievers" and announced the formation of a

religious army to counter the government called "Jaysh al-Mahdi" ("JAM") – the Mahdi Army.

351. JAM featured several attractive assets for Iran and Hezbollah, including a strong base of support among the poorest and most disenfranchised Shi'a communities, a network of mosques and social institutions, and a vast supply of young, desperate men. However, it was initially an unruly and unprofessional organization ill-suited to confronting an advanced military in the way Hezbollah had successfully attacked the Israel Defense Forces.

352. Hezbollah operatives were present on the ground in Iraq following the U.S. invasion in 2003 and were directly involved in providing training and support to JAM from its inception. Hezbollah operatives Imad Mughniyeh and Mustafa Badr al-Din worked closely both with Sadr and his associates and the Badr Organization at this time, but Hezbollah remained cautious and did not encourage either Badr or JAM to immediately attack Coalition Forces.

353. In 2008, Imad Mughniyah was killed in Syria.

354. Ten years after his death, several of his former protégés gathered at an elaborate ceremony to pay tribute to him and extol his contributions to the terror campaign he helped launch in Iraq.

355. At an event commemorating the anniversary of his death, on February 23, 2018, several Iraqi Shi'a notables spoke, including Abu Mahdi al-Muhandis, who declared: "The martyr Mughniyah is still present in all fields of confrontation as [part of] a jihadist school that terrorized the enemies...."

356. Qais Khazali (discussed below), also in attendance, asserted that: "The pillars of the Islamic Resistance that took place in Iraq were the fruit of the martyr Mughniyah."

357. He went on to say:

> I got to know him in 2003 or 2004. At that time when I met him, I didn't know that he is Imad Mughniyeh. I only knew him as "Haj Radwan."

> Imad Mughniyah was the person behind the Iraqi Resistance against the American occupation of Iraq. The first generation of the commanders of the Resistance were the product of the Mughniyah's training.

358. Although Mughniyah was a key figure in Hezbollah's operational activities in Iraq, its political and diplomatic role in guiding Iraqi Shi'a factions was of equal, if not greater, importance.

359. For this purpose, Hezbollah also tapped a senior member of its Political Council, Muhammad Kawtharani, to be responsible for the organization's Iraq portfolio. As the U.S. Treasury Department noted when it designated him an SDGT on August 22, 2013, Kawtharani was:

> [T]he individual in charge of Hizballah's Iraq activities, Kawtharani has worked on behalf of Hizballah's leadership to promote the group's interests in Iraq, including Hizballah efforts to provide training, funding, political, and logistical support to Iraqi Shi'a insurgent groups.

360. Kawtharani was an inspired choice because he not only previously lived in Iraq but had also been a pupil of Ayatollah Muhammad Sadiq al-Ṣadr.

361. Kawtharani wasted no time in contacting one of Sadr's most trusted deputies, Mustafa al-Yaqubi, soon after (and possibly before) the overthrow of the Hussein regime in 2003. Mustafa al-Yaqubi had frequent contact with Kawtharani through the years and appears to have served as a primary channel for communications between Hezbollah and Sadr and his JAM forces.

362. Hezbollah was the obvious and natural choice for implementing the IRGC's creation and sponsorship of JAM in Iraq. First, as noted above, Hezbollah operatives were, like the Iraqi Sadrists, ethnically Arabs and spoke Arabic, whereas the Iranian IRGC operatives were ethnically Persian and spoke Farsi. Second, there were many longstanding personal and intellectual connections between Hezbollah and the Sadrist Movement.

363. According to a 2007 MNF-I report, "members of the Sadr movement have deep

respect for Lebanese Hezbollah…. Hezbollah sends trainers to Iran to train Iraqi fighters on EFPs." For instance, Muqtada al-Sadr's father-in-law was Grand Ayatollah Muhammad Baqir al-Sadr, who was a contemporary of Hezbollah's spiritual leader, Muhammad Fadlallah. Hezbollah's leader, Hassan Nasrallah, received his religious education in Lebanon from a seminary that taught Baqir al-Sadr's teachings on Shi'ism.

364. From June 2003 through August 2004, at Iran's direction, Hezbollah's role was primarily to organize and train JAM gunmen and try to instill discipline and professionalism into the organization so that it could effectively threaten and attack U.S. and Coalition Forces in Iraq. Due to its conflict with Israel in Lebanon, Hezbollah possessed hard-earned specialized experience and expertise on how to deploy new tactical and technological countermeasures against a modern army.

365. By early 2005, the presence of Hezbollah operatives in Iraq became an open secret when Iraqi Interior Minister Falah al-Naquib announced the arrest of eighteen Lebanese Hezbollah members on terrorism charges.

366. The UK's *Belfast Telegraph* reported in 2007 that Muqtada al-Sadr publicly acknowledged his organization's coordination with Hezbollah: "Speaking in Tufa in Iraq, Muqtada al-Sadr, the head of the Mehdi Army, admitted to 'formal links' with Hizbollah. 'We have formal links with Hizbollah, we do exchange ideas and discuss the situation facing Shi'as in both countries,' he said. 'It is natural that we would want to improve ourselves by learning from each other. We copy Hizbollah in the way they fight and their tactics, we teach each other, and we are getting better through this.'"

C. THE DEVELOPMENT OF THE JAM SPECIAL GROUPS AND THE PROMISED DAY BRIGADES

367. A Sadrist uprising led by armed JAM forces in August 2004 in the Shi'a holy city of Najaf soon changed the direction of the conflict.

368. In Najaf, JAM forces confronted U.S. Marines on a large scale and suffered significant casualties. An estimated 1,500 JAM fighters were killed and an undetermined number, most likely in the thousands, were wounded. By comparison, over the course of same three-week period, the U.S. military lost 9 soldiers and Marines in Najaf.

369. IRGC-QF personnel were present during the bloodshed and carefully observed the fighting. The lesson the IRGC-QF gleaned from the Najaf uprising was clear—JAM members were too disorganized and undisciplined to cause any serious harm to Coalition Forces as then constituted.

370. Thus, shortly after the uprising in Najaf was brought under control, Muqtada al-Sadr reluctantly authorized his deputies to create what became known as the "Special Groups" to be supported and trained by Hezbollah and funded and controlled by the IRGC.

371. The IRGC wanted JAM to be able to deploy more professional (and lethal) forces that could successfully attack Coalition Forces in Iraq, while Sadr's "regular" JAM militia concentrated on ethnic cleansing and kidnapping Sunnis as well as its traditional criminal enterprises.

372. Initially, the Special Groups functioned essentially as regional commands – clusters of terror cells – under the overall leadership of Muqtada al-Sadr's senior deputies, including Qais al-Khazali and Akram al-Kaabi (a/k/a Akram Abbas al-Kabi). As the U.S. military later noted:

> When Special Groups were formed, [Qais Khazali] and Akram al Kabi were named the general supervisors, or members of the Ishraf Committee (Ishraf means oversight and supervision). Qais and Layth [Qais' brother] were

> directly involved with Special Groups, and in this position, they would negotiate and procure weapons and IEDs from Iran and distribute them to JAM.

373. This arrangement provided both a face-saving way for Sadr to retain overall control of his followers and a way for the IRGC-QF and Hezbollah to create, organize, oversee, and supervise terror cells under their operational control that could more effectively carry out IRGC and Hezbollah attacks against U.S. Forces.

374. From the initial formation of JAM's Special Groups in 2004 through much of 2006, the IRGC-QF used Hezbollah – and particularly, its Unit 3800 – to train and direct these cells (as well as parallel Badr Organization cells) to target Coalition Forces.

375. This was confirmed by Akram Kaabi himself during a January 1, 2019 interview on Al-Nujaba TV, a channel operated by Al-Nujaba, an Iranian-backed Shi'a group formed in 2013 as an outgrowth of Special Group Asa'ib Ahl al-Haq ("AAH") (discussed below) and designated (together with Kaabi) as an SDGT on March 5, 2019.

376. During the interview, Kaabi stated that:

> After [the 2004 Battle of Najaf], we realized that we needed a new method, especially since the brothers from Hezbollah and from the IRGC helped us in that battle in Najaf. Even in Sadr City, there were Iranian consultants. There was an IRGC officer called Abu Ali, who was originally from Ahwaz and spoke fluent Arabic. He was with us in Najaf, and he helped us with the battle management and provided much-needed basic and important advice.

377. He went on to say:

> Our chief engineer in Najaf, Dr. Jassem Al-Abadi, who was martyred, was among the first to be trained by that brother from Hizbullah and by the brothers from the IRGC. So, we realized that if we acquired more capabilities, things would improve. Our morale was high. Our mujahideen were ready to make sacrifices. So, we decided to take this path and acquire a lot of expertise. So, we developed our relationship with the brothers in Hizbullah and the IRGC. Both Hizbullah and the IRGC were open with us about everything...

378. Kaabi was also explicit about the degree to which his exploits in Iraq were directed and coordinated with Hezbollah's senior leadership:

> After the battle of Najaf, I traveled by land to Syria and then to Lebanon, and I met Hassan Nasrallah for the first time. The brothers [in Hizbullah] did not keep any secrets from us. They were forthcoming with their years of experience. They summarized this experience and presented it to us in full detail and this, indeed, led to a significant change in our resistance on the ground.
>
> The late Imad Mughniyah participated in my meeting [with Nasrallah]. Nasrallah and Mughniyah asked me to debrief them about the battle of Najaf – the events, and the deployment of the forces and the vehicles. Mughniyah even asked me to present everything on a blackboard so that they would get a feel for what had happened on the ground. So, I reviewed all the details. Nasrallah was... Obviously, all this happened in the second meeting. The first meeting was an official introductory meeting. Then, since I was still in Lebanon, the second meeting was held. Both Nasrallah and Mughniyah sympathized with us. Both said that they had tried to contact us many times prior to the events in Najaf and that had they succeeded we would have been able to accomplish greater victories, and to change the balance of power significantly. But they said that this was the will of the Lord and that Hezbollah will not deny us anything. They said: 'All of our capabilities and expertise are at your disposal.'

379. Perhaps most notable, the interview specifically discussed the role of EFPs in targeting American forces in Iraq:

> At first, we used old anti-aircraft missiles to manufacture IEDs. They would cause a large explosion, with a loud noise and lots of smoke, but they had little effect on the heavily armored [American] vehicles. Penetrating this armor was no easy task.
>
> But later, our IEDs improved. We started using explosively formed penetrators. These charges would not cause a lot of smoke or a loud explosion, but they would penetrate the armor of the tanks through a certain hole. They would explode inside the tank, destroying it and killing everyone inside.

380. Kaabi's narrative broadly confirms the intelligence assessment publicly disclosed over the past few years. In sum, the IRGC–QF instructed Hezbollah to create "Unit 3800," an entity dedicated to supporting Iraqi Shi'a terrorist cells targeting MNF–I.

381. Hezbollah also trained Special Groups and Badr Organization operatives at training camps in southern Lebanon and Iran.

382. From September 2004 to late 2005, these newly-formed Special Groups cells conducted low-intensity operations against the British and U.S. military, launching gradually increasing numbers of EFP attacks, and also training in Iran and Lebanon with Hezbollah and the IRGC-QF to develop and improve their TTPs while preparing for the next round of conflict.

383. As Special Groups members detained by Coalition Forces later explained, only Hezbollah instructors taught Special Groups operatives the "Engineers Course" that focused on the construction and employment of EFPs, and not every Special Group operative received this training.

384. One detainee reported that "Engineers are special and have to be smart. If you are not smart no one will waste the time and expenses to send you to Iran to train to be an engineer because you will fail."

385. Hezbollah also trained these "Engineers" on how to incorporate EFPs into the tactical design of ambushing Coalition Forces convoys, principally to kidnap Coalition soldiers. The tactics for a kidnapping-ambush using EFPs closely resembled the tactics Hezbollah developed in attempting to kidnap Israel Defense Forces soldiers in Southern Lebanon.

386. As one interrogation of a Detainee revealed:

> During one of [Detainee]'s training sessions, his group was instructed on techniques involving the attack of military convoys and abduction of POWs. Upon the arrival of a four-vehicle convoy, EFP's would be emplaced to disable the first three vehicles in a convoy. The attackers, who are hiding on one side of the road from an unidentified distance away, would successively fire upon the fourth vehicle with shoulder-fired missiles. Amidst the attack, two small groups of individuals would alternatively bound from the hidden area away from the road to the fourth vehicle while firing upon the fourth vehicle using small arms. The alternatively bounding small groups would advance to the vehicle, pull out any individual who is

> still living, and bring the individual back to an area where the attackers' own convoy of vehicles is waiting. In order to prevent a quick reaction force from arriving to aid the disabled convoys, a simultaneous mortar attack would be planned on a nearby military base. The simultaneous mortar attack would be followed through to keep the quick reaction force at the nearby base busy. Another way to prevent assistance from a quick reaction force would be to emplace more EFPs at a further distance down the same planned route as the military convoy. An attack combining an EFP and other methods of attacking a convoy is called a "complex attack."

387. For approximately two years, under Hezbollah's tutelage and with the support and oversight of the IRGC, JAM Special Groups carry out attacks against Coalition Forces at the direction of Hezbollah and the IRGC.

388. By 2007, MNF-I officials were reporting carefully planned, complex ambushes and retaliatory attacks on U.S. forces that included direct assaults on U.S. military outposts, ambushes in which American troops were captured and complex attacks that used multiple weapons to strike more than one U.S. target.

389. Hezbollah and the IRGC-QF also introduced the Special Groups to the use of 107mm and 122mm artillery rockets (frequently referred to as "Katyusha rockets") which Hezbollah had previously deployed in large numbers against the Israel Defense Forces in southern Lebanon and against Israeli border towns in northern Israel.

390. Both "regular" JAM and the Special Groups used these same types of artillery rockets in their indirect fire attacks on U.S. and Coalition Forward Operating Bases and MNF-I Headquarters in the Green Zone.

391. The IRGC also supplied JAM and JAM Special Groups with 240mm rockets (also known as the Fadjr-3) developed by the Shahid Bagheri Industries division of the Aerospace Industries Organization of Iran ("AIO").

392. Not only did the IRGC supply these weapons to both Hezbollah and (later) its Iraqi Shi'a proxies, but Hezbollah's TTPs in the use of these weapons were also transferred to JAM and the JAM Special Groups.

393. During a July 2, 2007 press briefing, General Bergner noted that Special Groups were trained in Iran by Hezbollah instructors in a four-week long course that was titled "Artillery." According to General Bergner, U.S. intelligence concluded that: "This course teaches the use of indirect fire weapons including 60mm and 120mm mortars, and 107mm, 122mm and 240mm rockets."

394. However, despite the increased tempo of Hezbollah-directed violence and improved lethality of the Special Groups, Sadr himself remained personally and politically erratic.

395. Because the Special Groups were designed to carry out attacks on Coalition Forces on Hezbollah's and the IRGC's behalf and as their proxies, Hezbollah and IRGC would not tolerate deviations from their overall direction or strategies.

396. Thus, while Hezbollah and the IRGC intensified the training of select operatives and cultivated Special Groups cell commanders, they gradually began peeling those cell commanders away from the Sadrist Movement (as discussed below).

397. For much of 2007-2008, Sadr was also embroiled in political disputes with rival Shi'a parties and "regular" JAM units engaged in violent clashes with the Badr Organization, including a very public clash in Karbala during a religious festival.

398. In June 2008, Sadr announced his intention to disband JAM to focus his organization on social, cultural and religious activities. But he soon further proclaimed that he would maintain an elite force, the Promised Day Brigades ("PDB"), to carry out attacks against Coalition Forces.

399. Although they had, by this time, directed their energies primarily into more disciplined Special Groups, Hezbollah and the IRGC were careful not to alienate Sadr.

400. Accordingly, the PDB received funding and weapons from the IRGC and training and direction from both Hezbollah and the IRGC.

401. PDB deployed many EFPs against American and Coalition Forces in Iraq after July 2008. In August 2009 alone, MNF-I attributed 15 EFP attacks in Baghdad to PDB.

402. MNF-I took significant and forceful measures against the PDB. However, because of the financial, logistical and operational support it received from both Hezbollah and the IRGC, the PDB was able to not only survive, but to continue to menace American forces in Iraq through 2011. For example, on June 28, 2011, the PDB issued a statement claiming responsibility for 10 mortar and Katyusha rocket attacks against U.S. military convoys in which U.S. officials confirmed that three U.S. troops were killed.

D. ASA'IB AHL AL-HAQ

403. The Asa'ib Ahl Al-Haq ("AAH," or the "League of the Righteous") terrorist organization began as a JAM Special Group, directed by Hezbollah and funded and armed by the IRGC-QF, that conducted numerous attacks on Coalition Forces—particularly on American targets—as well as Iraqi Security Forces.

404. AAH was originally established by senior JAM commander and later MNF-I detainee, Qais al-Khazali. Qais Khazali was a pupil of Muqtada al-Sadr's father and later one of Muqtada al-Sadr's senior deputies. But he also maintained an uneasy rivalry with the younger al-Sadr that occasionally devolved into open hostilities.

405. Khazali had accompanied Sadr to Tehran in 2003, and he maintained contact with senior IRGC-QF leadership when he assumed control of Special Groups cells after 2004.

According to a report by the U.S. military:

> In August 2006 MAS (Muqtada al-Sadr) asked [Qais al-Khazali] to lead a delegation to Tehran to discuss the situation in Iraq and Iranian support for JAM (Jaysh al-Mahdi (JAM) Militia subordinate to Muqtada al-Sadr). According to reporting, Ali Khamenei (Sayyid Ali Hosseini Khamenei was then and is still now the Supreme Leader of Iran) met with [Qais al-Khazali] and recruited him to lead a special group known as Asayb al-Haq [AAH], or the K2 network. The K2 network would operate with the knowledge or authorization of MAS. [Qais al-Khazali] agreed. Iran was interested in working with [Qais al-Khazali] because of his influence on MAS. Layth (al-Khazali's brother, captured with him on 20 March, 2007 in Basra, served as the Operations Chief for Asayb al-Haq) and as a liaison between the secret network formed by Qayis and the Iranians. In his position, Layth travelled frequently between Iraq, Iran and Syria.

406. Qais al-Khazali and his brother Layth al–Khazali returned to Iraq, requisitioned the most experienced and capable fighters from Sadr's JAM terror cells, and formed the new Special Group AAH.

407. At first, AAH appears to have remained within JAM's orbit, nominally under the umbrella of the Sadrist Movement, but it later emerged as a more cohesive group whose commanders were no longer pledged to Sadr, but to Hezbollah and the IRGC.

408. This likely resulted from assessments made by senior Hezbollah commanders, including Ali Musa Daqduq, who had travelled to Iraq at the IRGC-QF's behest to evaluate the training, organization and effectiveness of the Special Groups.

409. AAH formally split from JAM in 2007 (though it continued to maintain significant ties with JAM even later).

410. Hezbollah identified Qais Khazali and Akram Kaabi as among the more capable JAM Special Groups cell commanders.

411. Hezbollah cultivated them, and ultimately recruited them to serve as direct proxies of the IRGC-QF unbeholden to Sadr.

412. According to an April 2007 MNF-I report, Qais Khazali admitted that AAH received direct financing from the IRGC-QF.

413. Within months of Qais Khazali's formation of AAH, he provided the religious blessing for the Hezbollah-planned and orchestrated raid on the Provincial Joint Coordination Center ("PJCC") in Karbala on January 20, 2007 (for which the IRGC-QF provided funding and extensive logistical support). As discussed more fully below, the kidnapping and murder of five American soldiers during the operation led to a concerted effort to locate the perpetrators, and it eventually resulted in the capture of both Khazalis in March 2007.

414. Thereafter, despite the capture and detention of the Khazali brothers, AAH continued to function as a full-fledged terrorist organization because of the significant funding, training, and weapons it received from the IRGC-QF, and from the training and other cooperation it obtained from Hezbollah.

415. AAH was able to maintain a high-level offensive tempo from mid-2007 until the departure of U.S. forces at the end of 2011, when Qais Khazali emerged from U.S. detention to become one of Iraq's most important political leaders.

416. In sum, from 2006 to 2011, AAH operated as Iran's direct terror proxy targeting U.S. personnel at the direction of Hezbollah and the IRGC-QF. Iran harbored elements of its leadership (and their families), trained and supplied its operatives, and funded the AAH cells. Iran used Hezbollah to train and direct AAH to commit attacks on Americans in Iraq on its behalf.

417. AAH has conducted countless of attacks against U.S. and Iraqi forces, targeted kidnappings of Westerners and Iraqis, rocket and mortar attacks on the U.S. Embassy, murdered American and British soldiers, and assassinated Iraqi officials.

418. At all relevant times, AAH received its funding from Iran, and acted as an agent of

Iran's IRGC-QF and Hezbollah.

419. At a July 2, 2007 press briefing, General Bergner, spokesman for the MNF-I, noted:

> The Qods Force also supplies the special groups with weapons and funding of 750,000 to 3 million U.S. dollars a month. Without this support, these special groups would be hard pressed to conduct their operations in Iraq […] The Qods Force goal was to develop the Iraqi special groups into a network similar to the Lebanese Hezbollah. Special groups would be unable to conduct their terrorist attacks in Iraq without Iranian-supplied weapons and other support. Like Ali Musa Daqduq, Qais' [Khazali] main contact was [General Shahlai], the deputy commander for Qods Force Department of External Special Operations. Funding and training of the special groups started in 2004.

E. KATA'IB HEZBOLLAH ("KH")

420. Kata'ib Hezbollah ("KH") ("Hezbollah Brigades") was active in Iraq from 2007 to 2011. It was founded by Abu Mahdi al-Muhandis, a member of the Badr Corps and one of the IRGC-QF's senior operatives in Iraq. In the 1980s, al-Muhandis was a member of the Iraqi Da'wa Party, in which capacity he worked closely with the IRGC-QF and Lebanese Hezbollah.

421. KH's overall operations were run by Karim Ja'far Muhsin al-Ghanimi, described by the U.S. Treasury Department as "the overall leader of KH, which has used facilities in Iran to send weapons to Iraq." According to the U.S. government, "Ghanimi has organized KH military-related training in Iran from the IRGC-QF and Lebanese Hizballah. Ghanimi has sent money provided by the IRGC-QF to KH leaders in Iraq."

422. KH has functioned as Iran's premier terror proxy in Iraq and like other Special Groups, its fighters received training from the IRGC-QF and Hezbollah in guerilla warfare tactics and the use of explosives, as well as weapons like the RPG-29, EFPs, and the deployment of Katyusha rockets for indirect fire attacks on U.S. forward operating bases ("FOBs").

423. The IRGC-QF provided RPG-29 anti-armor weapons exclusively to KH.

424. RPG-29s constitute "weapons of mass destruction" as that term is defined in 18

U.S.C. § 2332a(c)(2)(A) and 18 U.S.C. § 921.

425. The IRGC-QF also provided IRAMs almost exclusively to KH. IRAMs are "flying IEDs" – explosive devices made from large metal canisters, such as propane gas tanks, filled with explosives, scrap metal and ball bearings, propelled into the air by rockets. IRAMs were "purpose-built" for one objective: being lobbed over walls and Hesco[27] barriers at short ranges, preventing interception by C-RAM defense systems[28] that were protecting Coalition Forces manning bases in Iraq.

426. IRAMs first appeared in southern Iraq in November 2007. Like other IEDs, IRAMs could be triggered remotely by radio control, or timed to detonate by a washing-machine timer. IRAMs could be launched from either a frame resting on the ground or mounted on the bed of a truck and were designed to cause catastrophic damage and inflict mass casualties.

427. But, notwithstanding the fact that portions of IRAMs were sometimes constructed from commonly-used "household" materials (such as, *e.g.*, propane tanks), they require the use of military-grade rockets, and their proper assembly required a high-degree of technical sophistication that KH obtained from Hezbollah and the IRGC-QF.

428. The first known IRAM attack in Iraq occurred at FOB Loyalty in Baghdad. Two American soldiers were killed and 16 wounded. A second attack in the Sha'ab neighborhood of Baghdad was the result of an accidental explosion of IRAMs likely intended for Combat Outpost

---

[27] Hesco barriers are a multi-cellular barrier system manufactured from welded zinc-aluminum coated steel wire mesh, joined with vertical, helical-coil joints, and lined with a heavy-duty non-woven polypropylene geotextile. Once filled with earth, sand, and dirt, the Hesco barriers provide exceptional protection against conventional fire attacks. *See* http://www.hesco.com/products/defensive-barriers/mil.

[28] Counter Rocket, Artillery, and Mortar, abbreviated "C-RAM" or "Counter-RAM," is a set of systems used to detect and/or destroy incoming artillery, rockets and mortar rounds in the air before they hit their ground targets, or simply provide early warning. *See* https://en.wikipedia.org/wiki/Counter_Rocket,_Artillery,_and_Mortar. *See also* https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/.

Callahan, approximately 800 yards away from where the truck carrying the IRAMs prematurely exploded, killing 18 civilians and wounding an additional 29.

429. IRAM attacks were particularly dangerous to Coalition Forces and had the potential to kill dozens in a single attack. Once launched, an incoming IRAM could not be stopped. A soldier spotting the approach of a suspected IRAM-bearing vehicle could have as little as "two seconds to decide whether the person emerging from it ha[d] just set it for firing or [was] simply an innocent driver getting out to change a tire."

430. IRAMs became a signature weapon of KH.

431. KH operated mainly in Shi'a areas of Baghdad, such as Sadr City, and throughout southeastern Iraq conducting (1) rocket-propelled grenade (RPG) attacks; (2) 107mm and 240mm rocket attacks; (3) IRAM attacks; and (4) EFP attacks on U.S. and Coalition Forces. KH was also supplied by Iran with its production model of the RPG-29 anti-tank rocket launcher.

432. This model RPG-29 was first used against U.S. forces during operations in Sadr City, Baghdad.

433. On June 24, 2009, the United States designated KH an FTO. The State Department explained that:

> The organization has been responsible for numerous violent terrorist attacks since 2007, including improvised explosive device bombings, rocket propelled grenade attacks, and sniper operations. Kata'ib Hezbollah [sic] also targeted the International Zone in Baghdad in a November 29, 2008 rocket attack that killed two UN workers. In addition, KH has threatened the lives of Iraqi politicians and civilians that support the legitimate political process in Iraq.

434. KH was also simultaneously designated an SDGT, because it was "responsible for numerous terrorist acts against Iraqi, U.S., and other targets in Iraq since 2007."

435. The U.S. Treasury Department also designated KH as an entity threatening stability

in Iraq pursuant to E.O. 13438. The Treasury Department's 2009 press release announcing KH's designation explained that KH had "committed, directed, supported, or posed a significant risk of committing acts of violence against Coalition and Iraqi Security Forces…."

436. The Treasury press release also stated: "[f]urther, the IRGC-Qods Force provides lethal support to Kata'ib Hizballah and other Iraqi Shia militia groups who target and kill Coalition and Iraqi Security Forces."

437. The 2009 press release further reported that:

> Between March 2007 and June 2008, Baghdad-based Kata'ib Hizballah cell members participated in multiple rocket-propelled grenade (RPG) and improvised rocket-assisted mortar (IRAM) attacks against U.S. forces. These attacks included a May 13, 2008 RPG-29 attack on a U.S. tank located in Sha'ab, Iraq, and a February 19, 2008 IRAM attack on a U.S. base near Rustamiya, Iraq. A February 19, 2008 rocket attack in the Rustamiya area resulted in one U.S. civilian killed and injuries to U.S. civilian and Coalition Forces personnel.
>
> As of 2008, Kata'ib Hizballah was funded by the IRGC-Qods Force and received weapons training and support from Lebanon-based Hizballah. In one instance, Hizballah provided training--to include building and planting IEDs and training in coordinating small and medium arms attacks, sniper attacks, mortar attacks, and rocket attacks--to Kata'ib Hizballah members in Iran.
>
> Recordings made by Kata'ib Hizballah for release to the public as propaganda videos further demonstrate that Kata'ib Hizballah conducted attacks against Coalition Forces. In mid-August 2008, Coalition Forces seized four hard drives from a storage facility associated with a Kata'ib Hizballah media facilitator. The four hard drives included approximately 1,200 videos showing Kata'ib Hizballah's sophisticated planning and attack tactics, techniques, and procedures, and Kata'ib Hizballah's use of the most lethal weapons--including RPG-29s, IRAMs, and EFPs--against Coalition Forces in Iraq.
>
> One of the hard drives contained 35 attack videos edited with the Kata'ib Hizballah logo in the top right corner. Additionally, between February and September 2008, Al-Manar in Beirut, Lebanon, broadcast several videos showing Kata'ib Hizballah conducting multiple attacks against Coalition Forces in Iraq.

> Immediately preceding the Government of Iraq's approval of the United States-Iraq security agreement in late November 2008, Kata'ib Hizballah posted a statement that the group would continue fighting Coalition Forces and threatened to conduct attacks against the Government of Iraq if it signed the security agreement with the United States.

438. In 2008, the U.S. Department of Defense described the linkages it found between KH, Iran and multiple terrorist attacks against Coalition Forces in Iraq—including KH's use of EFPs:

> [A]lso known as Hezbollah Brigades, [KH] is a terrorist group believed to receive funding, training, logistics and material support from Iran to attack Iraqi and coalition forces using what the military calls 'explosively formed penetrators' – roadside bombs designed to pierce armor-hulled vehicles – and other weapons such as rocket-assisted mortars.

439. As noted above—and as stated by the U.S Treasury Department in its July 2009 press release—throughout 2008, *Al-Manar*, Hezbollah's official television outlet in Lebanon (and itself a designated SDGT since May 2006), played numerous videos of KH launching rocket and IED/EFP attacks against U.S. troops. In this manner, Hezbollah helped publicize KH's activities and wage psychological warfare against the United States.

440. The U.S. Treasury Department designated KH's founder, Abu Mahdi al-Muhandis, an SDGT in July 2009 and announced the designation in the same press release announcing KH's designation. The press release noted:

> As of early 2007, al-Muhandis formed a Shia militia **group employing instructors from Hizballah** to prepare this group and certain Jaysh al-Mahdi (JAM) Special Groups for attacks against Coalition Forces. The groups received training in guerilla warfare, handling bombs and explosives, and employing weapons--to include missiles, mortars, and sniper rifles. In another instance as of September 2007, al-Muhandis led networks that moved ammunition and weapons--to include explosively formed penetrators (EFPs)--from Iran to Iraq, distributing them to certain JAM militias to target Coalition Forces. As of mid-February 2007, al-Muhandis also ran a weapons smuggling network that moved sniper rifles through the Iran-Iraq border to Shia militias that targeted Coalition Forces.

> Al-Muhandis also provided logistical support for attacks against Iraqi Security Forces and Coalition Forces conducted by JAM Special Groups and certain Shia militias. In one instance, in April 2008, al-Muhandis facilitated the entry of trucks--containing mortars, Katyusha rockets, EFPs, and other explosive devices--from Iran to Iraq that were then delivered to JAM Special Groups in Sadr City, Baghdad. Additionally, al-Muhandis organized numerous weapons shipments to supply JAM Special Groups who were fighting Iraqi Security Forces in the Basrah and Maysan provinces during late March-early April 2008.
>
> In addition to facilitating weapons shipments to JAM Special Groups and certain Shia militias, al-Muhandis facilitated the movement and training of Iraq-based Shia militia members to prepare them to attack Coalition Forces. In one instance in November 2007, al-Muhandis sent JAM Special Groups members to Iran to undergo a training course in using sniper rifles. Upon completion of the training course, the JAM Special Groups members had planned to return to Iraq and carry out special operations against Coalition Forces. Additionally, in early March 2007, al-Muhandis sent certain Shia militia members to Iran for training in guerilla warfare, light arms, marksmanship, improvised explosive devices (IED) and anti-aircraft missiles to increase the combat ability of the militias to fight Coalition Forces.
>
> In addition to the reasons for which he is being designated today, al-Muhandis participated in the bombing of Western embassies in Kuwait and the attempted assassination of the Emir of Kuwait in the early 1980s. Al-Muhandis was subsequently convicted in absentia by the Kuwaiti government for his role in the bombing and attempted assassination. (Emphasis added.)

441. In a July 2010 press briefing, U.S. General Ray Odierno identified KH as the group behind increased threats to U.S. bases in Iraq. General Odierno confirmed that KH operatives had gone to Iran for special training and then returned to Iraq. General Odierno stated, "[T]hey are clearly connected to Iranian IRGC [Iranian Revolutionary Guard Corps]."

442. In sum, from 2007 to 2011, KH operated as Iran's direct terror proxy targeting U.S. personnel at the direction of Hezbollah and the IRGC-QF. Iran harbored elements of its leadership (and their families), trained and supplied its operatives, and funded the KH cells. Iran used Hezbollah to train and direct KH to commit attacks on Americans in Iraq on its behalf.

F. CASE IN POINT: SENIOR HEZBOLLAH COMMANDER ALI MUSA DAQDUQ'S DIRECTION OF TERRORIST ATTACKS ON COALITION FORCES IN IRAQ

443. In March 2007, Ali Musa Daqduq was captured in Basra, Iraq.

444. At the time of his arrest, he produced identification indicating his name was Hamid Muhammad Jabur Al Lami and that he was a mute. Only during further questioning did he admit to being part of Lebanese Hezbollah and acknowledge his ability to speak.

445. In 2005, Hezbollah's leader, Hassan Nasrallah, had tapped Daqduq to work for Unit 3800, and in May 2006, Daqduq traveled to Tehran with Yusuf Hashim, a fellow Hezbollah operative and senior supervisor of Hezbollah operations in Iraq. There they met with General Shahlai, Deputy Commander of the IRGC-QF Special External Operations. Daqduq was directed to return to Iraq and report on the training and operations of the JAM Special Groups and provide assessments on their training in mortars and rockets, use of IEDs (particularly EFPs) and kidnapping operations.

446. As MNF-I investigators later learned, Daqduq not only provided training to AAH cells and advised them on terrorist operations, he also helped plan operations and had final approval over them. Daqduq reported to Hashim, and the latter reported to Hezbollah's Muhammad Kawtharani and General Shahlai.

447. Daqduq conducted multiple visits to Iraq to undertake training needs assessments, survey the operational environment, and obtain feedback from JAM Special Groups members in Iraq on their needs. This was intended to ensure that the training being designed and staffed by Hezbollah instructors would provide the greatest benefit to their students.

448. In addition, Daqduq's assessments provided informed feedback to the IRGC-QF logisticians on the armaments the JAM Special Groups fighters needed to meet their needs and

improve their operational performance.

449. In early 2007, in his capacity as a senior Hezbollah commander, Daqduq planned, authorized, and directed an attack on U.S. service members in the PJCC in Karbala. Pursuant to his direction, on January 20, 2007, a team of at least 12 AAH gunmen, disguised as U.S. soldiers, infiltrated the PJCC in Karbala. In the well-planned attack, they killed one U.S. soldier and abducted four others, whom they later executed.

450. Two months later, when Coalition Special Forces captured Qais al-Khazali, his brother Layth al-Khazali, who led the attack, and Daqduq in Basra, the documents, computers and media recovered from capture, as well as the subsequent interrogations of these men, significantly supplemented the U.S. military's understanding of Hezbollah's operational role in Iraq and the IRGC-QF's central role in supporting and enabling the JAM Special Groups.

451. Amongst the documents recovered was a 22-page memorandum written by Daqduq that "detailed the planning, preparation, approval process and conduct of the [Karbala] operation," as well as Daqduq's role in overseeing other Special Groups operations.

452. As noted in a Memorandum for Commander, Multi-National Force—Iraq, dated May 31, 2007:

> [Daqduq] has knowledge of Iranian surrogate networks operating in Iraq and has admitted to meeting Iranian Revolutionary Guard Corps-Quds Force (IRGC-QF) personalities on multiple occasions including Hajj Yusif, who is assessed to be Abdul Reza Shahlai, the Department 9000 (Lethal Aid) Deputy Commander.

453. According to U.S. military officials, both Daqduq and Qais Khazali admitted that senior leadership within the IRGC-QF knew of and helped plan the attack on the Karbala PJCC, and Daqduq served as the liaison between the IRGC-QF, Hezbollah and AAH.

454. For example, a May 22, 2009 memorandum summarizing the interrogations of Daqduq noted:

> [Daqduq] is a Lebanese Hizballah Commander and was an advisor to AAH leadership. [Daqduq] was involved in the planning of the Karbala PJCC attack in January 2007 and the reconnaissance of various CF bases and ports. [Daqduq] took his direction from IRGC-QF Officer Hajji Yusif [General Shahlai] and LH [Lebanese Hezbollah] Unit 2800 Commander Yusif Hashim.

455. An August 13, 2007 Memorandum recounted the data retrieved from the Basra location of the March raid:

> The hard drives contained numerous insurgent related documents and photographs, including a journal detailing upcoming operations or meetings; 'how to' manuals on operating arms/munitions systems—including various missiles and RPG launchers; old US military training materials; photographs of MNF equipment and resources; Google Earth aerial photographs of regions and cities in Iraq; photographs of U.S. service members performing their jobs; photographs of destroyed U.S. military equipment; photographs of an unknown shipyard; photographs of a destroyed MNF dining facility; and, propaganda videos by ISI showing missile testing, dead bodies, and destroyed vehicles. Of note, photographs were also found of items from the wallet of [3.5(c)] a U.S. soldier killed in a complex attack on the Provincial Joint Coordination Cell in Karbala on 20 Jan 07—including his SSA card, credit cards, identification cards, and family photographs. Documents seized include: spreadsheets detailing weapons and targets; step-by-step instructions for operations/attacks; and numerous letters equivalent to after-action reports detailing attacks.

456. An October 5, 2008 Memorandum further noted:

> [Daqduq] admitted to being Lebanese Hezbollah and admitted to an active role in Iraq as an agent of Iranian state-sponsored terrorism. [Daqduq] admitted that Abdul Reza Shahlai, Iranian Revolutionary Guard Corps - Quds Force (IRGC-QF) Department 9000 (Lethal Aid) Deputy Chief facilitated [Daqduq]'s illegal entry into Iraq on four separate occasions. IRGC-QF is one of the primary agents of Iranian state sponsored terrorism. [Daqduq] admitted that his role was to arrange for training of Shi'a extremist groups, facilitating training and weapons procurement for Special Groups. Special Groups have conducted numerous AIF [Anti-Iraqi Forces] and ACF [Anti-Coalition Forces] attacks throughout Iraq. [Daqduq] admitted to a significant operational planning role in the abduction and murder of 5 U.S. Service Members.

457. Khazali described Daqduq as the "designer of the Special Groups."[29] The exploitation of a computer that was captured during the raid revealed contents that confirmed the training and evaluation role that Daqduq performed. "Documents seized include: spreadsheets detailing weapons and targets, step-by-step instructions for operations/attacks; and numerous letters equivalent to after-action reports detailing attacks, including, for example: an ambush and IED attack on a MNF convoy in Karbala resulting in 4 X MNF KIA; an IED attack on a British patrol which destroyed two Land Rovers and killed the occupants; and a sniper attack on a British patrol which killed a British soldier."

458. For example, Daqduq was found in possession of training manuals on tactics for launching rocket attacks.

459. In his personal journal, Daqduq recorded: "Met with the brothers the observers of Diyalah province and I listened regarding operations … We conducted eight explosive charge operations on both sides."

460. U.S. intelligence also learned about Hezbollah's series of 30-day training courses held for Iraqi Special Groups. These included:

- Engineering: This is a demolitions course, focusing on the construction and emplacement of EFPs, including the use of Passive Infra-Red devices or "Magic Eye."
- Artillery: This course teaches the use of indirect fire weapons, including 60mm and 120mm mortars, and 107mm, 122mm, and 240mm rockets.
- Intelligence: This class covers basic source operations and collection, observations, etc. to derive intelligence that is used at the tactical level.

461. According to U.S. intelligence, Hezbollah also conducted "mini-courses" and "refresher training" at a camp near Tehran and also taught a course for JAM Special Groups on

[29] Ali Musa Daqduq was held in U.S. detention until November 2011 with the goal of extraditing him to the U.S. for trial. The Iraqi Government denied the request, and he was transferred to Iraqi custody on December 18, 2011. The charges that the U.S. had brought against him were summarily rejected by an Iraqi Court in May 2012 as lacking evidence and he was released from confinement, later returning to Lebanon.

how to improve their "kidnapping capability."

462. According to U.S. intelligence estimates, following Daqduq's 2007 arrest, the IRGC-QF provided Hezbollah and Daqduq up to $3 million in U.S. currency every *month* to run JAM Special Groups in Iraq.

463. Ultimately, the U.S. military concluded that Daqduq's mandate was "to reorganize the Special Groups into an organization that mirrored Lebanese Hizbollah."

464. On November 19, 2012, the U.S. Department of the Treasury designated Ali Musa Daqduq an SDGT pursuant to Executive Order (E.O.) 13224, and noted:

> Daqduq is a senior Hizballah commander responsible for numerous attacks against Coalition Forces in Iraq, including planning an attack on the Karbala Joint Provincial Coordination Center (JPCC) on January 20, 2007, which resulted in the deaths of five U.S. soldiers.
>
> On March 20, 2007, Coalition Forces in southern Iraq captured Daqduq, who falsely claimed to be a deaf mute at the time and produced a number of false identity cards using a variety of aliases. From January 2009 until December 2011, U.S. military forces held Daqduq in Iraq under the terms of the 2008 "Agreement Between the United States of America and the Republic of Iraq on the Withdrawal of United States Forces from Iraq and the Organization of Their Activities during Their Temporary Presence in Iraq" (the Security Agreement). In December 2011, the United States transferred Daqduq to Iraq's custody in accordance with our obligations under the Security Agreement. He was subsequently tried in Iraq on terrorism and other charges. On May 7, 2012, an Iraqi court dismissed terrorism and false documents charges against him. Daqduq remained in Iraqi custody until last week when the Iraqi government determined that it no longer had a legal basis to hold him, and he was released Friday.

G. IRAN FUNDED THE DESIGN AND PRODUCTION OF EXPLOSIVELY FORMED PENETRATORS ("EFPS") USED TO KILL OR MAIM HUNDREDS OF U.S. SERVICE MEMBERS

465. As noted above, the EFPs deployed by the IRGC and Hezbollah in Iraq were not truly "improvised" explosive devices but professionally manufactured and specifically designed to target U.S. and Coalition Forces' armor.

466. EFPs constitute "weapons of mass destruction" as that term is defined in 18 U.S.C. § 2332a(2)(A).

467. First used by Hezbollah against Israeli armor in Lebanon, EFPs are categorized by the U.S. military as a type of shaped-charge weapon. They are usually made by placing a precision-manufactured concave copper disk in front of high-explosives that have been packed into a steel tube with a cap welded to one end.

468. In Iraq, EFPs were often triggered by a passive infra-red devices that ultimately set off an explosion within the steel casing of the EFP, forcing the copper disk forward, and turning it into a high-velocity molten slug that could pierce the military-grade armor of most U.S. vehicles deployed in Iraq.

469. To produce these weapons, copper sheets are often loaded onto a punch press to yield copper discs. These discs are annealed in a furnace to soften the copper. The discs are then loaded into a large hydraulic press and formed into the disk-like final shape.

470. This munitions manufacturing process is critical to the design and concomitant lethality of the EFP weapon.

471. Unlike homemade explosive devices such as traditional IEDs, EFPs are far more sophisticated and are specifically designed to target vehicles such as armored patrols and supply convoys, though Hezbollah and its Special Groups proxies have deployed them against U.S. and Iraqi civilians as well.

472. Because Iran propagated its specialized weapons knowledge up and down its network of terror proxies in Iraq, the U.S. State Department's 2006 Country Reports on Terrorism further documented Iran's specific efforts to provide terrorists with lethal EFPs to ambush and murder U.S. and other Coalition Forces:

> Iran provided guidance and training to select Iraqi Shia political groups, and weapons and training to Shia militant groups to enable anti-Coalition attacks. Iranian government forces have been responsible for at least some of the increasing lethality of anti-Coalition attacks by providing Shia militants with the capability to build IEDs with explosively formed projectiles similar to those developed by Iran and Lebanese Hezbollah. The Iranian Revolutionary Guard was linked to armor-piercing explosives that resulted in the deaths of Coalition Forces. The Revolutionary Guard, along with Lebanese Hezbollah, implemented training programs for Iraqi militants in the construction and use of sophisticated IED technology. *These individuals then passed on this training to additional militants in Iraq.* (Emphasis added.)

473. Also, in 2006, Brigadier Gen. Michael Barbero, Deputy Chief of Staff for Strategic Operations of MNF-I stated: "Iran is definitely a destabilizing force in Iraq. I think it's irrefutable that Iran is responsible for training, funding and equipping some of these Shi'a extremist groups and also providing advanced IED technology to them, and there's clear evidence of that."

474. That same year, the Deputy Chief of Staff for Intelligence with the MNF-I, U.S. Army Major General Richard Zahner, declared that:

> Labels on weapons stocks seized inside and outside Iraq point to Iranian government complicity in arming Shiite militias in Iraq […] Iran is funneling millions of dollars for military goods into Iraq […] You'll find a red label on the C-4 [explosive] printed in English and will tell you the lot number and name of the manufacturer.

475. Major General Zahner further added:

> [T]he control of military-grade explosives in Iran is controlled through the state apparatus and is not committed through rogue elements right there. It is a deliberate decision on the part of elements associated with the Iranian government to affect this type of activities.

476. General Bergner commented on Iran funding Hezbollah operatives in Iraq:

> Actions against these Iraqi groups have allowed coalition intelligence officials to piece together the Iranian connection to terrorism in Iraq […] Iran's Quds Force, a special branch of Iran's Revolutionary Guards, is training, funding and arming the Iraqi groups. […] It shows how Iranian operatives are using Lebanese surrogates to create Hezbollah-like

> capabilities. And it paints a picture of the level of effort in funding and arming extremist groups in Iraq.

477. General Bergner further noted that:

> The groups operate throughout Iraq. They planned and executed a string of bombings, kidnappings, sectarian murders and more against Iraqi citizens, Iraqi forces and coalition personnel. They receive arms—including explosively formed penetrators, the most deadly form of improvised explosive device—and funding from Iran. They also have received planning help and orders from Iran.

478. In May 2007, the Commander of the Multi-National Division-Center, U.S. Army Major General Richard Lynch, stated that:

> Most of our casualties have come from improvised explosive devices. That's still the primary threat to our soldiers—IEDs. And we have an aggressive campaign to counter those IEDs, but they still are taking a toll on our soldiers: 13 killed, 39 soldiers wounded. *What we're finding is that the technology and the financing and the training of the explosively formed penetrators are coming from Iran.* The EFPs are killing our soldiers, and we can trace that back to Iran." [Emphasis added.]

479. According to the U.S. State Department's 2007 Country Reports on Terrorism:

> Despite its pledge to support the stabilization of Iraq, Iranian authorities continued to provide lethal support, including weapons, training, funding, and guidance, to some Iraqi militant groups that target Coalition and Iraqi security forces and Iraqi civilians. In this way, Iranian government forces have been responsible for attacks on Coalition forces. The Islamic Revolutionary Guard Corps (IRGC)-Qods Force, continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, mortars that have killed thousands of Coalition and Iraqi Forces, and explosively formed projectiles (EFPs) that have a higher lethality rate than other types of improvised explosive devices (IEDs), and are specially designed to defeat armored vehicles used by Coalition Forces. The Qods Force, in concert with Lebanese Hezbollah, provided training outside Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry. These individuals then passed on this training to additional militants inside Iraq, a "train-the-trainer" program. In addition, the Qods Force and Hezbollah have also provided training inside Iraq. In fact, Coalition Forces captured a Lebanese Hezbollah operative in Iraq in 2007.

480. Other U.S. Government reports, such as the Department of Defense's 2007 *Measuring Stability and Security in Iraq* quarterly report to Congress, similarly concluded that:

> The Iranian regime's primary tool for exercising clandestine influence in Iraq is the Islamic Revolutionary Guard Corps' (IRGC) Qods Force (QF), which provides arms, intelligence, funds, training, and propaganda support to Iraqi Shi'a militants targeting and killing Coalition and Iraqi forces, as well as Iraqi civilians. The QF seeks to increase long-term Iranian strategic influence in Iraq and the withdrawal of U.S. forces. Among the weapons it provides to Iraqi militants are improvised explosive devices (IEDs), advanced IED technologies (including explosively formed projectiles (EFPs)), and rockets and mortars used for indirect fire attacks.

481. These observations continued in 2008.

482. According to the U.S. State Department's 2008 Country Reports on Terrorism:

> The Qods Force, an elite branch of the Islamic Revolutionary Guard Corps (IRGC), is the regime's primary mechanism for cultivating and supporting terrorists abroad. The Qods Force provided aid in the form of weapons, training, and funding to HAMAS and other Palestinian terrorist groups, Lebanese Hezbollah, Iraq-based militants, and Taliban fighters in Afghanistan.…
>
> Despite its pledge to support the stabilization of Iraq, Iranian authorities continued to provide lethal support, including weapons, training, funding, and guidance, to Iraqi militant groups that targeted Coalition and Iraqi forces and killed innocent Iraqi civilians. Iran's Qods Force continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, and mortars that have killed Iraqi and Coalition Forces as well as civilians. Tehran was responsible for some of the lethality of anti-Coalition attacks by providing militants with the capability to assemble improvised explosive devices (IEDs) with explosively formed projectiles (EFPs) that were specially designed to defeat armored vehicles. The Qods Force, in concert with Lebanese Hezbollah, provided training both inside and outside of Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry.

483. One of the ways in which the IRGC provided "militants with the capability to assemble improvised explosive devices (IEDs) with explosively formed projectiles (EFPs) that were specially designed to defeat armored vehicles" included providing them with manufacturing

supplies such as copper and steel, as well as machinery—including hydraulic presses used to form copper into the shape of disks used in EFPs.

484. Likewise, the State Department's 2011 Country Reports on Terrorism reported:

> Despite its pledge to support the stabilization of Iraq, Iran continued to provide lethal support, including weapons, training, funding, and guidance, to Iraqi Shia militant groups targeting U.S. and Iraqi forces, as well as civilians. Iran was responsible for the increase of lethal attacks on U.S. forces and provided militants with the capability to assemble explosives designed to defeat armored vehicles. The IRGC-QF [Islamic Revolutionary Guard Corps-Quds Force], in concert with Lebanese Hezbollah, provided training outside of Iraq as well as advisors inside Iraq for Shia militants in the construction and use of sophisticated improvised explosive device technology and other advanced weaponry.

485. Similarly, in 2011, the U.S. Ambassador to Iraq, James F. Jeffrey, was quoted as saying:

> [F]resh forensic testing on weapons used in the latest deadly attacks in the country bolsters assertions by U.S. officials that Iran is supporting Iraqi insurgents with new weapons and training. […] We're not talking about a smoking pistol. There is no doubt this is Iranian.

486. All of the foregoing support from Iran and its agents for attacks on Coalition Forces and Iraqi civilians was financed and facilitated, in substantial part, by funds transfers initiated by Iran through Iranian banks (including, *inter alia*, the Central Bank of Iran, Bank Melli Iran and Defendant Bank Saderat Plc) on behalf of, and for the benefit of, the IRGC, Hezbollah and IRISL as part of the Conspiracy set forth in detail herein.

487. Because of the size and scope of Iran's efforts to murder Americans in Iraq—and subvert the U.S.-sponsored and freely elected Iraqi government—Iran required access to hundreds of millions of dollars that it could only reliably and effectively transfer through the global financial system with the illicit assistance of the Western Bank Defendants.

H. THE ATTACK AT ISSUE IN THIS COMPLAINT WAS AN ACT OF INTERNATIONAL TERRORISM

488. At no time relevant to this Action did the United States declare war or enact an Authorization for the Use of Military Force against Iran.

489. At no time relevant to this Action did the United States engage in an armed conflict with the military forces of Iran, or Iran's military forces or their agents engage in lawful acts of war against Coalition Forces.

490. At no time relevant to this action did Hezbollah's and the IRGC's agents in Iraq who killed and injured Coalition Forces and civilians carry fixed distinctive signs recognizable at a distance, carry arms openly, conduct their operations in accordance with the laws and customs of war, or enjoy any form of combatant immunity for their acts.

491. The specific attack alleged herein was committed by Hezbollah and the IRGC-QF through their terror KH cells in Iraq, not by armed forces of recognized governments or military forces.

492. The injuries Plaintiffs sustained were not the result of, nor did they occur in the course of, a declared war with Iran, or an armed conflict between the United States and Iran.

493. The conduct of Iran, the IRGC and Hezbollah violated the laws of armed conflict (including, *e.g.*, AAH operatives masquerading as members of U.S. armed forces and executing defenseless prisoners), and the attacks upon Iraqi and other civilians constituted a substantial, rather than an incidental, part of their objectives and conduct.

494. The acts of the IRGC and Hezbollah that injured the Plaintiffs were acts of international terrorism within the meaning of 18 U.S.C. § 2331, involving violent acts intended to influence the United States by coercion (by coercing the withdrawal of Coalition Forces from Iraq) and to intimidate and coerce the Iraqi population, and were also acts constituting terrorist activities

within the meaning of 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or engaging in terrorism within the meaning of 22 U.S.C. § 2656f.

495. At all relevant times Hezbollah was (and remains) a designated Foreign Terrorist Organization.

496. From October 25, 2007 to the present, the IRGC-QF has been an SDGT (and an FTO in 2019). The IRGC was also designated an SDGT in 2017 and an FTO in 2019.

VII. OVERVIEW OF THE CONSPIRACY

A. AGREEMENT AND KNOWLEDGE

497. As noted above, "the Conspiracy" identified in this Amended Complaint first began in the years immediately after Iran was first designated by the United States as a State Sponsor of Terrorism in 1984.

498. As a result of that designation, Iran developed various ways to circumvent U.S. economic sanctions levied against the regime and to facilitate the free movement of U.S. dollars that Iran obtained (largely from the sale of petroleum and natural gas) without detection by the U.S. government in order to pursue foreseeably illicit objectives, including:

a. Concealing hundreds of billions of dollars of Iran's U.S. dollar-denominated transactions from detection, scrutiny, or monitoring by U.S. regulators, U.S. law enforcement, and/or U.S. depository institutions;

b. Assisting Iran in transferring at least $150 million to the IRGC-QF, Hezbollah, the Special Groups, and other instruments of Iranian state-sponsored terrorism; and

c. Assisting Iran in acquiring technology and components for its illegal Weapons of Mass Destruction program and illicit conventional arms trade.

499. To further those objectives, Iran enlisted several Iranian state-owned banks as well as Defendant Bank Saderat Plc and various international financial institutions, including the

Western Bank Defendants in this Action, which agreed to alter, falsify, or omit information from payment order messages that involved Iran or Iranian parties, in particular several Iranian banks (as noted above, referred to herein occasionally as the "Iranian Bank Co-conspirators" (including Defendant Bank Saderat Plc)), as well as IRISL, for the express purpose of concealing Iran's financial transactions in the Eurodollar market from detection, scrutiny, or monitoring by U.S. regulators, law enforcement, and/or depository institutions.

500. The Conspiracy between Iran, the IRGC and its agents (including NIOC), IRISL, Defendant Bank Saderat Plc, the other Iranian Bank Co-conspirators, and the Western Bank Defendants began no later than 1987, and upon information and belief, continues to the present (though individual Defendants joined the Conspiracy at different dates).

501. The Conspiracy orchestrated by Iran made it possible for Iran to transfer: (1) hundreds of billions in U.S. dollar-denominated funds from its Eurodollar accounts maintained by various international banks, including the Defendants, through the United States in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies; and (2) hundreds of millions of dollars to Hezbollah, the IRGC, and other terrorist organizations actively engaged in murdering and maiming U.S. servicemen and civilians in Iraq.

502. Each of the Defendants knowingly entered into an agreement with Iran and its agents, including but not limited, to Defendant Bank Saderat Plc, other Iranian Bank Co-conspirators, including but not limited to, the Central Bank of Iran, Bank Melli (including Bank Melli's United Kingdom subsidiary Melli Bank Plc), and Bank Sepah (which are all instrumentalities of Iran), as well as the IRGC-controlled IRISL, under which the conspirators agreed to alter, falsify, or omit information from payment order messages for USD-denominated Eurodollar, trade-finance, precious metals and foreign exchange transactions that were

purposefully directed at, and processed through, the United States.

503. As alleged in detail below, each Defendant committed numerous overt acts in furtherance of the Conspiracy and knowingly and unlawfully agreed to engage in "stripping" hundreds of millions – and in some cases, billions – of U.S. dollar-denominated transactions on behalf of Iran knowing that Iran was a designated State Sponsor of Terrorism.

504. Each Defendant entered into its agreement with Iran and the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc) aware that other co-conspirators (either the Defendants herein, or other foreign financial institutions) were also actively participating in the Conspiracy, and shared the common goal of the scheme's purpose of providing Iran and the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc) with the ability to illegally transfer billions of dollars (undetected) through the United States, and were aware of many of the (often same or similar) methods being used by other members of the Conspiracy to effectuate it.

505. Accordingly, each Defendant understood that its conduct was part of a larger scheme engineered by Iran; each Defendant knew the participation of other conspirators was essential to the Conspiracy's success; and each Defendant knew of and joined in the overriding scheme and sought to achieve and facilitate a common goal of helping Iran transfer billions of dollars through the United States while avoiding detection, scrutiny, or monitoring by U.S. regulators, U.S. law enforcement, and/or U.S. depository institutions.

506. In addition, each Defendant also knew, or was deliberately indifferent to, several of the Conspiracy's foreseeable purposes and criminal objectives that included:

a. Facilitating illicit transactions totaling at least $50 million USD for the benefit of Hezbollah;

b. Facilitating illicit transactions totaling at least $100 million in USD funds for the direct benefit of the IRGC and billions in USD funds for the benefit of the NIOC, then controlled by the IRGC;

c. Facilitating at least hundreds of illicit transactions totaling more than $60 million on behalf of IRISL including over 150 "stripped" transactions after IRISL was designated an SDN;

d. Facilitating tens of millions of dollars in illicit transactions on behalf of MODAFL, the IRGC, Mahan Air and other instrumentalities of Iranian state sponsored terror to further numerous violations of the U.S. trade embargo against Iran, conceal Iran's efforts to evade U.S. sanctions and enable Iran's acquisition from the United States of goods and technologies prohibited by U.S. law to be sold or transferred to Iran, including components of IEDs deployed against Coalition Forces in Iraq; and

e. Enabling Iran, the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc), the IRGC, Hezbollah, and the Special Groups to plan for, conspire to, and perpetrate acts of international terrorism under 18 U.S.C. § 2331(1); homicides, attempted homicides, or conspiracies to commit homicide under 18 U.S.C. § 2332(a)-(c); bombings using destructive devices under 18 U.S.C. § 2332a; bombings and attempted bombings under 18 U.S.C. § 2332f; engaging in terrorist activity under 8 U.S.C. § 1189(a)(3)(B)(iii)-(iv); and/or engaging in terrorism under 22 U.S.C. § 2656f.

507. As set forth below, each of the Defendants knew that Iran was a U.S.-designated State Sponsor of Terrorism, and that U.S. laws and regulations required it to fully disclose all funds transfers through the United States made on behalf of Iran, Iranian entities and Iranian banks.

508. Despite that knowledge, each of the Defendants knowingly conspired with Iran and its agents (including Defendant Bank Saderat Plc) to violate those U.S. laws and regulations to conceal hundreds of millions (and in some cases, billions) of dollars in funds transfers routed through the Eurodollar correspondent banking network for clearance and settlement in the United States on behalf of Iran, IRISL, and the Iranian Bank Co-conspirators, including Defendant Bank Saderat Plc.

509. During the relevant time period from 2004 through 2011, and as set forth in greater detail herein, each of the Defendants knowingly agreed to join the Conspiracy; knowingly and

willfully participated in the Conspiracy; knew or was deliberately indifferent to the Conspiracy's criminal purposes and objectives; took initiatives to improve its workings; and was aware of the participation of many (if not all) of its members.

B. ACTS AND EFFECTS

510. Through the Conspiracy, Iran provided material support to Hezbollah, the IRGC and their Iraqi proxies, including the Special Groups, which targeted American citizens in Iraq, and with substantial assistance from the Western Bank Defendants, concealed and disguised the nature, location, source, and origin of the material support it provided to these terrorists, knowing and intending that the funds be used in preparation for and in carrying out acts of terrorism against Americans and others, including civilians, in Iraq.

511. As part of the Conspiracy, each of the Defendants took affirmative steps to violate U.S. criminal laws and to conceal from U.S. depository institutions, law enforcement, regulators, bank auditors, and counter-terrorism agencies the flow of hundreds of millions (and in some cases, billions) of U.S. dollars it was clearing and settling in the United States, including transfers for the benefit of the IRGC and Hezbollah, and through them to KH and other terrorist organizations actively engaged in murdering and maiming U.S. servicemen and civilians in Iraq on the IRGC's and Hezbollah's behalf.

512. The conduct of each Defendant, its awareness of other Defendants' and Co-conspirators' participation and conduct, and the resulting "glaring hole" in America's counter-financing of terrorism and sanctions architecture described by former Manhattan District Attorney Robert M. Morgenthau, provided Iran with vital access to the U.S. financial system.

513. U.S. "dollar clearing and settlement" – primarily (in this case) through the Clearing House Interbank Payments System in New York ("CHIPS-NY") system and the Federal Reserve

Bank of New York ("FRB-NY") – is an elaborate inter-bank system in the U.S. by which banks clear and settle credits and debits in their Eurodollar accounts with other banks all across the globe on a daily basis.

514. The U.S. "dollar clearing and settlement" system is critical not only to the workings of the global economy, but it also provides financial institutions (and nation states) with critical, essential access to global trade-finance credit denominated in U.S. dollars.

515. Thus, once Iran gained clandestine access to the U.S. "dollar clearing and settlement" system in New York, it could not only launder billions of dollars through its accounts in the Eurodollar market, but it could also borrow against the Eurodollar deposits it held in the Defendants' banks – facilitating further undetected transactions around the world in USD – both for ordinary commercial purposes and the illegal aims and objectives of the Conspiracy.

516. This broad-based access to the U.S. "dollar clearing and settlement" system was essential to Iran because of the scope of Iran's global ambitions at the time, which included driving the United States and its Coalition partners out of Iraq, dominating that country, and acquiring Weapons of Mass Destruction.

517. Thus, among the effects of the Conspiracy, a State Department diplomatic cable from March 2008 noted that:

> Bank Melli and the Central Bank of Iran also provide crucial banking services to the Qods Force, the IRGC's terrorist supporting arm that was headed by UNSCR 1747 designee Commander Ghassem Soleimani. Soleimani's Qods Force leads Iranian support for the Taliban, Hezbollah [sic], Hamas [sic] and the Palestinian Islamic Jihad. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least $100 million to the Qods Force. Bank Melli use of Deceptive Banking Practices … When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank

> Melli has requested that its name be removed from payment instructions for US dollar denominated transactions.

518. In addition, absent the access to the U.S. "dollar clearing and settlement" system afforded to Bank Saderat by the HSBC Defendants, Defendants SCB, Barclays, Credit Suisse and Commerzbank, both Iran and Hezbollah's access to USDs would have been diminished, and Iran's efforts to transfer large sums of U.S. dollars to Hezbollah would have been substantially impaired.

519. By knowingly agreeing to enter into the Conspiracy, and by knowing or being deliberately indifferent to its lethal purposes, and by committing multiple overt acts in furtherance of the Conspiracy, the Defendants provided Iran with the means by which it could transfer more than $150 million to the IRGC, Hezbollah and the Special Groups, which were actively engaged in planning and perpetrating the murder and maiming of hundreds of Americans in Iraq during the same period of time that the Conspiracy was proceeding, thereby substantially enhancing the ability of Iran, the IRGC, Hezbollah, and the Special Groups to inflict the deaths and injuries described herein.

520. The Conspiracy was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries because the Conspiracy substantially assisted Iran, the IRGC, IRISL, Mahan Air, Hezbollah, and/or the Special Groups in committing the acts of international terrorism that injured the Plaintiffs herein, by providing them collectively with more than $200 million U.S. dollars in funding that were used, *inter alia*, to arm, train and fund Iranian terror proxies in Iraq that targeted American citizens.

521. By knowingly agreeing to enter the Conspiracy, and participating in and committing overt acts in the course of the Conspiracy that resulted in damage and injury to the Plaintiffs, Defendants committed acts of international terrorism as defined by 18 U.S.C. §§ 2331, 2339A and 2339B that caused injury to the Plaintiffs in this action, and are civilly liable under 18

U.S.C. § 2333(a) of the Anti-Terrorism Act to the Plaintiffs, American citizens who have been injured by reason of acts of international terrorism perpetrated by Iran through its agents, including the IRGC, Hezbollah, and the Special Groups.

522. Defendant HSBC-US not only knowingly participated in the Conspiracy, but as a U.S. person within the meaning of 18 U.S.C. § 2332d also committed further acts of international terrorism in violation of 18 U.S.C. §§ 2331 and 2332d by knowingly (or with reason to know) facilitating financial transactions with Iran, which it knew was a designated State Sponsor of Terrorism. HSBC-US's acts were a cause of the injuries sustained by the Plaintiffs in this action, and HSBC-US is therefore civilly liable under 18 U.S.C. § 2333(a) of the ATA to the Plaintiffs.

523. Defendants SCB, ABN Amro (RBS N.V.), and Commerzbank not only knowingly participated in the Conspiracy, but because their respective New York branches constitute U.S. persons within the meaning of 18 U.S.C. § 2332d, these Defendants also committed further acts of international terrorism in violation of 18 U.S.C. §§ 2331 and 2332d by knowingly (or with reason to know) facilitating financial transactions with Iran, which each such Defendant knew was a designated State Sponsor of Terrorism. Those acts were a cause of the injuries sustained by the Plaintiffs in this action, and these Defendants are therefore civilly liable under 18 U.S.C. § 2333(a) of the ATA to the Plaintiffs.

C. BANK SADERAT PLC's AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

524. On September 8, 2006, the U.S. Office of Foreign Assets Control ("OFAC") amended § 560.516 of the ITRs and excluded Bank Saderat from the Iranian U-Turn exemption.

525. In announcing the 2006 change to the ITRs excluding Bank Saderat Iran from the U-Turn exemption, OFAC stated:

> OFAC has amended the Iranian Transactions Regulations (ITR) to cut off

> Bank Saderat, one of Iran's largest government-owned banks, from the U.S. financial system. Bank Saderat has been a significant facilitator of Hezbollah's financial activities and has served as a conduit between the Government of Iran and Hezbollah….

526. According to then-Under Secretary for Terrorism and Financial Intelligence Stuart Levey, "Bank Saderat facilitates Iran's transfer of hundreds of millions of dollars to Hezbollah and other terrorist organizations each year. We will no longer allow a bank like Saderat to do business in the American financial system, even indirectly."

527. The Treasury Department press release announcing the changes to the ITR stated that "a Hezbollah-controlled organization [] has received $50 million directly from Iran through Bank Saderat since 2001."

528. Assistant Treasury Secretary for Terrorist Financing Daniel Glaser testified before the Senate Committee on Banking, Housing and Urban Affairs that "Hezbollah uses Saderat to send money to other terrorist organizations as well."

529. For many years preceding the revocation of its U-Turn exemption, Bank Saderat illegally routed its USD transactions through the United States with the assistance of various Western commercial banks, including the Defendants herein.

530. From 2002 forward, Defendant Bank Saderat Plc continued Bank Saderat's existing practice of: (1) illegally routing its USD transactions through the United States; and (2) transferring tens of millions of dollars to Hezbollah and other designated terrorist groups.

531. As detailed in a January 9, 2009, Deferred Prosecution Agreement entered into by Lloyds TSB Bank Plc ("Lloyds") with U.S. law enforcement, Defendant Bank Saderat Plc directed illegal funds transfers to the U.S. and worked with Lloyds to strip its USD transactions of any reference to Iran or Bank Saderat.

532. In 2003, Lloyds exited its relationship with Bank Saderat Plc, and Defendant Credit

Suisse assumed Lloyds' role of illegally transferring USD through the United States while stripping references to Bank Saderat Plc and Iran from the transactions (as set forth below and, as also discussed below, in a Deferred Prosecution Agreement that Defendant Credit Suisse signed in 2009).

533. Notwithstanding the revocation of its access to the Iranian U-Turn exemption, Bank Saderat (and Bank Saderat Plc) continued to illegally direct USD transactions through the United States with the active assistance of the other Defendants listed herein.

534. On February 13, 2004, Defendant SCB opened accounts for Bank Saderat Plc. It also maintained other accounts for Bank Saderat Iran, including an account at SCB, Dubai.

535. During the relevant time period from 2004 to 2011, and as described in more detail below, Bank Saderat Plc, working in concert with Standard Chartered Bank, financed the illegal acquisition of various U.S.-origin export-controlled goods on behalf of Mahan Air and various sub-agencies of MODAFL.

536. For example, Standard Chartered Bank facilitated at least 10 transactions involving Letters of Credit valued at $1,559,127, which involved the shipment of U.S.-origin export-controlled aircraft parts sold by the Singapore-based Monarch Aviation, a company that was part of Iran's illegal procurement network, to various MODAFL sub-agencies.

537. A sub-agency of MODAFL obtained a Letter of Credit issued by Bank Refah, Iran, and sent it to Standard Chartered's branch in Singapore (where the Iranian front company Monarch Aviation maintained accounts) while reimbursement authorization was sent to the Iran Overseas Investment Bank London, i.e. Bank Saderat Plc's predecessor, which in turn either directly

financed the illegal acquisition of goods from the United States, or provided a surety for Bank Refah's payment.[30]

538. The goods were shipped by Iran Air[31] from Kuala Lumpur Airport, Malaysia, to Tehran Airport, Iran.

539. The LCs were refinanced by Standard Chartered's Dubai branch through its credit facility with the CBI, with payment being made to Monarch Aviation's account with Standard Chartered, Singapore through the latter's U.S. dollar account with Standard Chartered Bank, London, which in turn received the funds into its USD nostro account with Standard Chartered's New York branch.

540. In another instance discussed *infra*, Bank Saderat Plc knowingly sent a concealed and illegal payment via Standard Chartered's New York branch and JP Morgan Chase, New York, to Standard Chartered Bank in Dubai on behalf of a MODAFL's subsidiary, the Iran Helicopter Support and Renewal Company ("IHSRC").

541. The payment facilitated IHSRC's acquisition (via a company named Jetpower) of U.S. manufactured helicopter parts through an elaborate money laundering scheme intended to conceal from U.S. authorities: (1) the unlawful acquisition of U.S.- manufactured equipment for Iran's military; (2) the complex layering of the transaction involving Bank Melli's branches in London and Hong Kong; and (3) Bank Refah and Bank Saderat's involvement with SCB.

---

[30] The Reimbursing Bank usually pays the Negotiating Bank (in this case SCB) against a valid reimbursement authority received from the Issuing Bank (in this case Bank Refah) and a validated statement from the Negotiating Bank that the documents complied with LC terms, but in certain cases it only serves as a surety for the payment. SCB-London was also one of Bank Refah's correspondent banks in the UK.

[31] Iran Air was designated by the U.S. Treasury Department in 2011: "Iran's national airline carrier, Iran Air, is a commercial airline used by the IRGC and Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) to transport military related equipment.… Iran Air has provided support and services to MODAFL and the IRGC through the transport and/or transfer of goods for, or on behalf of, these entities. On numerous occasions since 2000, Iran Air shipped military-related electronic parts and mechanical equipment on behalf of MODAFL."

542. The HSBC Defendants also maintained one or more accounts for Bank Saderat Plc during the relevant time period.

543. In an October 9, 2006 email, Defendant HSBC-Middle East's Regional Head of Legal and Compliance noted the U.S. government's "direct evidence against Bank Saderat particularly in relation to the alleged funding of Hezbollah" but nonetheless maintained the account(s) thereafter and continued to facilitate transactions for Bank Saderat Plc.

544. As noted *supra*, in October 2007, Bank Saderat Iran (including Defendant Bank Saderat Plc), was designated an SDGT pursuant to E.O. 13224.

545. The U.S. Treasury Department's press release regarding Bank Saderat's designation stated:

> Bank Saderat, its branches, and subsidiaries: Bank Saderat, which has approximately 3200 branch offices, has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and EU-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad. For example, from 2001 to 2006, Bank Saderat transferred $50 million from the Central Bank of Iran through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence.

546. As set forth below, Defendant Barclays closed its Eurodollar accounts for Bank Saderat Plc, in 2008, months *after* Bank Saderat Plc was designated an SDGT, and more than a year after the U.S. Treasury Department reported that "Bank Saderat facilitates Iran's transfer of hundreds of millions of dollars to Hezbollah and other terrorist organizations each year."

547. The HSBC Defendants, and Defendants Commerzbank, SCB, Barclays, and Credit Suisse altered, falsified, or omitted information from Eurodollar payment order messages that they facilitated on behalf of Bank Saderat (and Bank Saderat Plc) at all times knowing, or deliberately indifferent to the fact, that Bank Saderat was facilitating Iranian-sponsored terrorism and, after October 2007, knowing, or deliberately indifferent to the fact, that Bank Saderat (including Bank

Saderat Plc) was an SDGT so-designated for its very role as a "significant facilitator of Hezbollah's financial activities and has served as a conduit between the Government of Iran and Hezbollah."

548. Moreover, as a Lebanese-based terrorist organization, Hezbollah was (and remains) particularly in need of USD funds because much of the Lebanese economy is "dollarized" (*i.e.* banking and retail transactions, credit and debt instruments are often, if not primarily, conducted in USD funds).

549. Accordingly, Bank Saderat Plc's provision of tens of millions of dollars to Hezbollah provided Hezbollah with substantial assistance in carrying out its terrorist activities in Iraq, including Hezbollah's commission of the terrorist attack that injured the Plaintiffs.

550. Moreover, Plaintiffs' injuries herein were a reasonably foreseeable result of Bank Saderat Plc's provision of tens of millions of dollars to Hezbollah.

D. THE CENTRAL BANK OF IRAN'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

551. The Central Bank of Iran ("CBI") is fully controlled and run by individuals directly appointed by the Government of Iran.

552. At all relevant times, the CBI has not functioned in the same manner as central banks in Western countries that are institutionally designed to be independent from political interference, nor is its purpose limited to "regulating" Iranian banks and managing Iran's currency and internal interest rates.

553. Instead, the CBI is an alter-ego and instrumentality of the Iranian government and its Supreme Leader, and it has routinely used Iranian banks like Bank Melli Iran and Bank Saderat Iran as conduits for terror financing and weapons proliferation on behalf of the Iranian regime.

554. At all relevant times, the CBI was an active participant in the Conspiracy.

555. For example, leading up to the adoption of UN Security Council Resolution 1747

(March 2007), which resulted in the freezing of assets belonging to Iran's Bank Sepah, the CBI furthered the Conspiracy by using non-Iranian financial institutions to shield Bank Sepah's assets from the impact of impending sanctions.

556. Throughout the relevant time period, the CBI maintained Eurodollar accounts at Bank Melli Iran, Bank Melli Plc, Bank Saderat Iran and Defendant Bank Saderat Plc in various currencies, including USD.

557. Bank Melli Iran's U.K. subsidiary (later Bank Melli Plc) managed the CBI's Eurodollar accounts in Europe.

558. In the wake of U.S. and later European Union designations against Iranian banks (including Bank Saderat and Bank Melli), the CBI often acted as a secret proxy for those designated entities.

559. As part of the Conspiracy, the CBI utilized Defendant Bank Saderat Plc to transfer USD funds to Hezbollah.

560. The CBI also maintained Eurodollar accounts, and unlawfully transferred USD funds in furtherance of the Conspiracy, with the assistance of Defendants SCB, ABN Amro (RBS N.V.) and the HSBC Defendants, including facilitating billions of dollars in USD funds transfers on behalf of the IRGC, through the aforementioned NIOC, which was designated as an SDN by the United States because it was an IRGC agent during the relevant time period.

561. As such, illicit transfers on behalf of the NIOC at that time were not for the benefit of a legitimate agency, operation or program of Iran.[32]

[32] The Superseding Indictment filed in *U.S. v. Zarrab* (filed in the S.D.N.Y (1:15-cr-00867)) demonstrates that NIOC continued to participate in the Conspiracy and launder U.S. dollars through U.S. financial institutions in 2013.

562. In addition, the Iran Threat Reduction and Syria Human Rights Act 2012 stated that:

> It is the sense of Congress that the National Iranian Oil Company and the National Iranian Tanker Company are not only owned and controlled by the Government of Iran but that those companies provide significant support to Iran's Revolutionary Guard Corps and its affiliates.[33]

563. Moreover, according to a published report, the National Iranian Oil Company even took an active role in support of Iran's terrorist activities in Iraq by providing intelligence in support of attacks against Coalition Forces along the Iranian border by using its own helicopters to conduct surveillance on Coalition Forces' FOBs.

564. In early 2001, and in furtherance of the Conspiracy, the CBI asked Defendant Standard Chartered Bank to act as its correspondent bank with respect to Eurodollar payments on behalf of the NIOC.

565. As alleged herein, SCB agreed to participate in the Conspiracy and remove identifying data on SWIFT-NET messages for these and other wire transfers.

566. Thereafter, between 2001 and 2006, the CBI sent approximately 2,226 payment order messages for a total value of *$28.9 billion* to Standard Chartered in London, the vast majority of which were illegally routed through the U.S. as described herein.

567. During the same time period, the CBI also maintained a Eurodollar credit facility at Standard Chartered Bank's branch in Dubai, UAE, which it used to assist Iran in illegally acquiring technology and components on behalf of MODAFL.

568. As detailed further below, and in furtherance of the Conspiracy, the CBI and Defendant ABN Amro (RBS N.V.) (which also maintained Eurodollar accounts for the CBI and

---

[33] *See*, https://www.treasury.gov/resource-center/sanctions/Documents/hr_1905_pl_112_158.pdf.

had numerous financial and business dealings with the CBI) conspired to provide illegal material support to Iran and Iranian parties.

569. Between 2002 and 2004, Defendant ABN Amro (RBS N.V.) accepted USD Eurodollar deposits from the CBI on a regular basis with an average deposit size in the range of $200 million USD, and the CBI instructed ABN Amro (RBS N.V.) to follow illegal procedures to launder USD-denominated Eurodollar deposits to the CBI's Eurodollar and local currency accounts with other European banks with branches or offices in London. ABN Amro (RBS N.V.) did so.

570. In furtherance of the Conspiracy, the CBI coordinated with Defendant ABN Amro (RBS N.V.)'s Central Bank Desk in Amsterdam regarding the procedure to be followed for repayment of USD deposits to their Eurodollar accounts with European banks with offices or branches in London.

571. This procedure stipulated that payment order messages sent to U.S. clearing banks for payment of USD funds to the CBI should not contain *any* reference to the Central Bank of Iran, or *any other* reference relating to Iran.

572. In 2001, the CBI also approached members of the HSBC Group, specifically Defendants HSBC-Middle East and HSBC-London, to obtain their agreement to move the CBI's clearing and settlement business from National Westminster Bank Plc to the HSBC Defendants, and intended to clear USD funds transactions through Defendant HSBC-US.

573. Pursuant to that agreement, the CBI eventually moved its Eurodollar accounts to the HSBC Defendants, and by late 2003, the CBI was one of six Iranian banks that used members of the HSBC Group for (mostly illegal) correspondent banking through the U.S. dollar clearing and settlement in New York.

574. With Defendant HSBC Holdings' knowledge, and in furtherance of the Conspiracy, Defendants HSBC-Middle East and HSBC-London manually intervened in the processing of payment orders by the CBI by removing: the Central Bank of Iran's name; its SWIFT-NET account (identified by BIC address BMJIIRTH); and country of origin (Iran).

575. Defendant HSBC-US also knew that other HSBC Defendants were altering and omitting information in SWIFT-NET payment order messages regarding Iranian parties, *i.e.* "stripping" these transactions, but nevertheless knowingly continued processing transactions despite that very knowledge.[34]

E. BANK MELLI IRAN AND MELLI BANK PLC'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

576. Bank Melli Iran, one of the largest banks in Iran, was established in 1927 by order of the Iranian Parliament.

577. Following the Iranian Revolution in 1979, all banks in Iran were nationalized, and even today most are effectively controlled by the Iranian regime.

578. Melli Bank Plc in London, England, was established in January 2002 as a wholly owned subsidiary of Bank Melli Iran.

579. According to the U.S. government, from 2004 to 2011, Bank Melli Iran and Melli Bank Plc in London transferred approximately $100 million USD to the IRGC-QF, which trained, armed, and funded terrorist groups that targeted, killed and maimed American and Iraqi forces and civilians.

---

[34] In furtherance of the Conspiracy, the CBI also conducted illegal precious metals transactions, primarily in gold bullion. For example, the December 2012 Consent Order entered into between OFAC and Defendant HSBC Holdings Plc stated that:

> On May 24, 2006, the London branch of HBUS acted as a clearing bank in a book entry transfer of 32,000 ounces of gold bullion, valued at $20,560,000, for the ultimate benefit of Bank Markazi, Iran [the CBI], in apparent violation of the prohibition against the "exportation . . . , directly or indirectly, from the United States, ... of any ... services to Iran or the Government of Iran," 31 C.F.R. § 560.204.

580. Specifically, according to the U.S. government in a November 10, 2009 diplomatic cable:

> [The] Islamic Revolutionary Guards Corps (IRGC) and IRGC-Qods Force, who channel funds to militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians, have used Bank Melli and other Iranian banks to move funds internationally. Bank Melli used deceptive banking practices to obscure its involvement from the international banking system by requesting that its name be removed from financial transactions when handling financial transactions on behalf of the IRGC.

581. Bank Melli Iran and Melli Bank Plc were designated as SDNs pursuant to E.O. 13382 in October 2007, and included on OFAC's SDN list, which resulted in, *inter alia*, their exclusion from the U-Turn exemption for Iranian Eurodollar transactions.

582. The U.S. Treasury Department press release announcing the designation stated:

> Bank Melli also provides banking services to the [Iranian Revolutionary Guard Corps] and the Qods Force. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least $100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from financial transactions.

583. In April 2008, Assistant Treasury Secretary for Terrorist Financing Daniel Glaser testified before the House Committee on Foreign Affairs, Subcommittee on the Middle East and South Asia and the Subcommittee on Terrorism, Nonproliferation and Trade, confirming that:

> Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least $100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from financial transactions.

584. The October 24, 2019 Section 311 Designation of Iran as a "Jurisdiction of Primary Money Laundering Concern" stated that:

> Bank Melli was among those banks designated pursuant to E.O. 13224 for assisting in, sponsoring, or providing financial, material, or technological support for, or other services to or in support of, the IRGC-QF. As of 2018, the equivalent of billions of USD in funds had transited IRGC-QF controlled accounts at Bank Melli. Moreover, Bank Melli had enabled the IRGC and its affiliates to move funds into and out of Iran, while the IRGC-QF, using Bank Melli's presence in Iraq, had used Bank Melli to pay Iraqi Shia militant groups.

585. In mid-2007, Bank Melli Iran's branch in Hamburg ("Bank Melli-Hamburg") transferred funds for the Defense Industries Organization ("DIO").

586. DIO is an Iranian government-owned defense manufacturer whose name, logo and/or product tracking information was stamped on munitions found in weapons caches that were seized from the Special Groups in Iraq; including large quantities of weapons produced by DIO in 2006 and 2007 (for example, 107 millimeter artillery rockets, as well as rounds and fuses for 60 millimeter and 81 millimeter mortars.)

587. Since at least the mid-1980s, Bank Melli has maintained Eurodollar accounts, at one time or another, with Defendants ABN Amro (RBS N.V.), Barclays, Credit Suisse, SCB, Commerzbank and the HSBC Defendants.

588. As early as 1987, Bank Melli instructed Defendant Barclays to process Eurodollar transactions in favor of Bank Melli's London branch by referencing only Bank Melli's Eurodollar account number at Midland Bank Plc in London without referencing Bank Melli Iran's name in the SWIFT-NET payment orders.

589. Bank Melli further instructed Barclays to send separate payment order message instructions, which included full transaction details, to Bank Melli's London Branch.

590. Barclays agreed and assisted Bank Melli in its illegal conduct and continued to do so even *after* Bank Melli was designated by the United States and publicly identified as a major source of the IRGC's funding.

591. No later than December 2000, Bank Melli opened a Eurodollar account with Defendant ABN Amro (RBS N.V.)'s branch in Dubai, United Arab Emirates ("UAE") and worked with ABN Amro (RBS N.V.) to strip its U.S. dollar-denominated transactions.

592. Similarly, in July 2003, Defendant SCB learned that a competitor was exiting the Iranian business completely and sought to pick up this business and add Eurodollar accounts for five Iranian banks at SCB-London. Bank Melli was among the banks whose business SCB expressly sought to (and did) acquire.

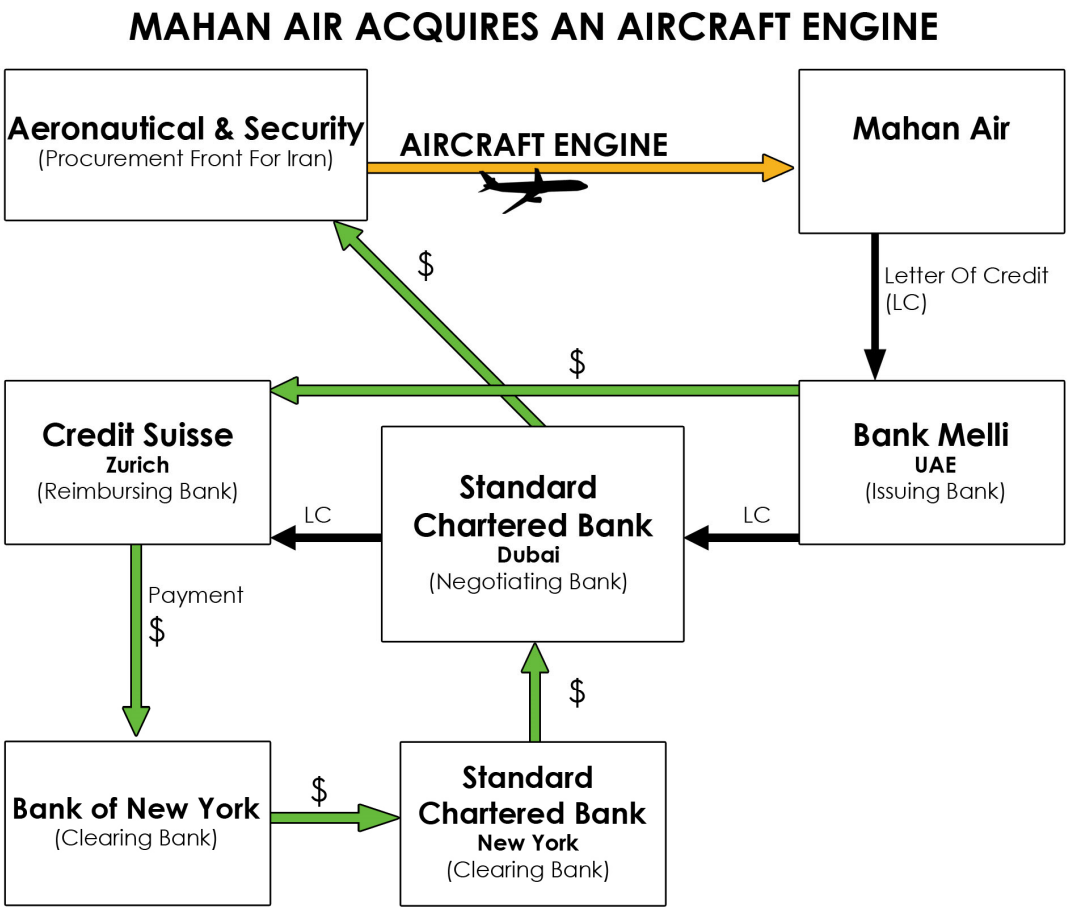
593. In January 2004, SCB decided to proceed with the Iranian business, and no later than February 13, 2004, SCB opened Eurodollar accounts for Bank Melli and thereafter participated in the Conspiracy by facilitating unlawful transactions for Bank Melli.

594. In addition, Bank Melli Iran's branch in the UAE was instrumental in facilitating U.S. sanctions-evading trade-finance and Eurodollar payment transactions on behalf of Mahan Air and MODAFL.

595. For example, Bank Melli issued a Letter of Credit to Mahan Air in August 2004 through Standard Chartered Bank, Dubai in favor of a UAE-based company called Aeronautical & Security for the shipment of an aircraft engine (identified by model number CF6-50C2) manufactured by General Electric and shipped from Luxemburg to Tehran, Iran.

596. Bank Melli UAE instructed Credit Suisse, Zurich to make the payment, which in turn instructed Bank of New York in New York (one of Credit Suisse's U.S. clearing and settlement banks) to credit SCB's New York branch for further credit to the account of SCB-Dubai, which then credited Aeronautical & Security's Eurodollar account.

597. The following flow-chart shows the overall flow of USD funds involved with Mahan Air's illegal acquisition of a U.S.-manufactured, export-controlled aircraft engine:



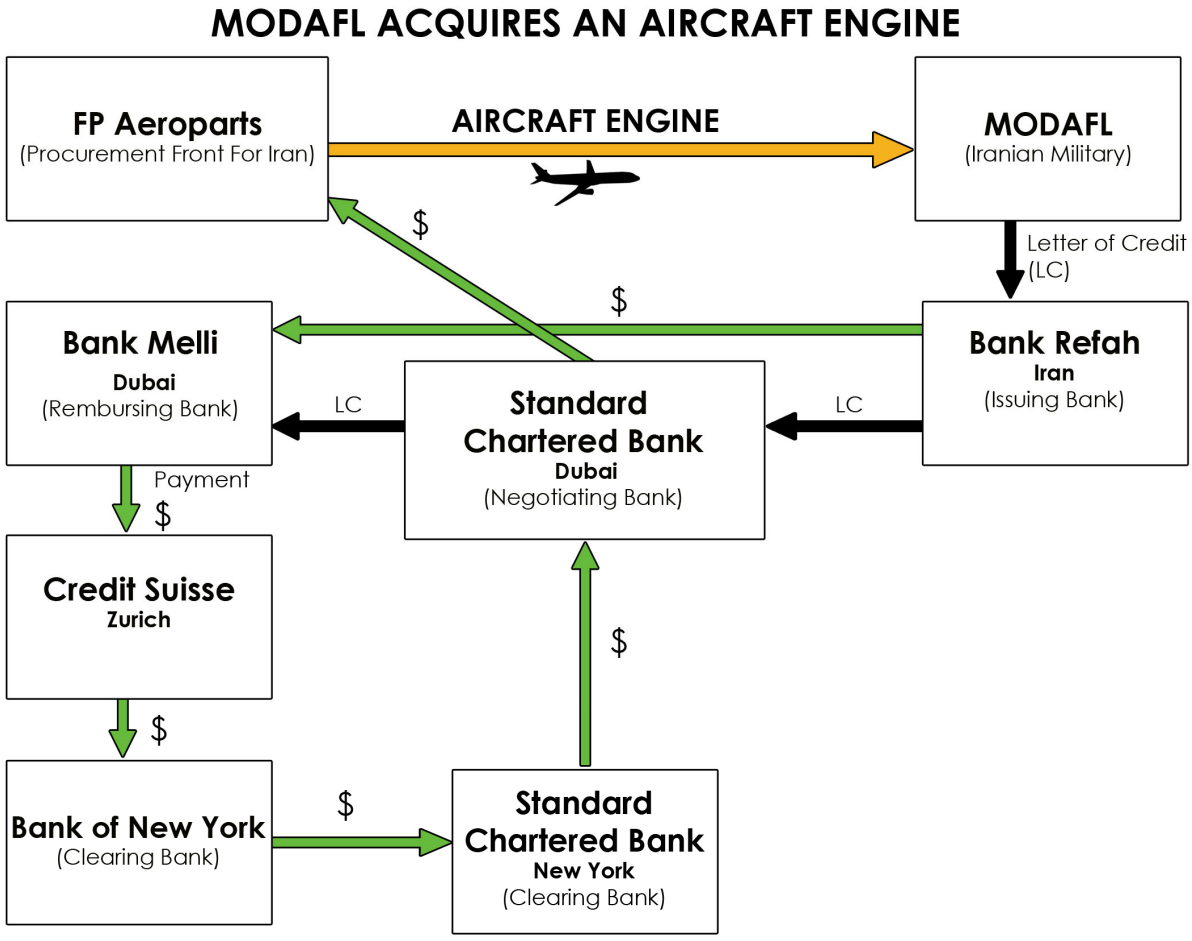
598. In another example, Bank Refah Kargaran, Iran issued a Letter of Credit in USD to a MODAFL sub-agency through Standard Chartered Bank, Dubai in favor of a Dubai-based company called FP Aeroparts for the illegal shipment (via Iran Air) of U.S. aircraft parts.

599. Bank Melli served as the Reimbursing Bank on the trade-finance transaction, and it subsequently instructed Credit Suisse, Zurich to debit its Eurodollar account as part of the flow of USD funds between the LCs counterparties.

600. As the LC transaction proceeded, Credit Suisse then further instructed The Bank of New York to pay Standard Chartered Bank's New York branch (the clearing bank for the transaction), which further credited the USD account it maintained for SCB, Dubai with the amount due for the shipment of aircraft parts.

601. To close-out the LC transaction, SCB, Dubai then credited the Eurodollar account it maintained on behalf of FP Aeroparts Middle East for the amount of the shipment.

602. The following flow-chart shows the overall flow of USD funds involved with MODAFL's illegal acquisition of the U.S.-manufactured aircraft parts:



603. As reflected in the above flow-chart, and during the relevant time period, Defendant Credit Suisse maintained Eurodollar accounts in Zurich, Switzerland on behalf of Bank Melli.

604. Credit Suisse also instructed and trained Bank Melli employees, and conspired with Bank Melli, on ways to format Bank Melli's payment orders so that the resulting SWIFT-NET

messages would avoid detection by the automated filter algorithms in U.S. depository institutions' automated OFAC sanction screening software.

605. During the relevant time period (and beginning no later than July 2003), Defendant Commerzbank also conspired with Bank Melli to route its Eurodollar clearing and settlement business through Commerzbank's correspondent banking relationships and SWIFT-NET accounts.

606. Commerzbank further advised Bank Melli to list "non ref" in the ordering party field in all payment order messages because it would trigger a manual review of the overall Eurodollar payment transaction, thereby enabling Commerzbank personnel to ensure that the SWIFT-NET messages did not contain any information linked to Iran.

607. Defendant HSBC-London also maintained Eurodollar accounts for Bank Melli Iran, and it used HSBC-US to provide illegal USD funds clearing and settlement services for Bank Melli during the relevant period.

608. Yet despite the fact that several SWIFT-NET payment order messages were supposed to have been fully "stripped" by HSBC-London—before their transmittal to the U.S.—they were nevertheless blocked by the HSBC-US OFAC filter in New York because Bank Melli was referenced in error (thus placing HSBC-US on notice that HSBC-London was working in concert with Bank Melli to evade U.S. law, regulations and economic sanctions against Iran).

609. Even with these blatant warning signs, HSBC-US continued to routinely provide Eurodollar clearing and settlement services to the HSBC Defendants, knowing full well that they were violating U.S. laws and regulations by laundering money on behalf of Bank Melli.

610. Because, as discussed below, HSBC-US knew of this unlawful conduct—and continued to facilitate it— HSBC-US violated, *inter alia*, 18 U.S.C. § 2332d.

F. BANK MELLAT'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

611. Bank Mellat provides banking services in support of Iran's Weapons of Mass Destruction program through the Atomic Energy Organization of Iran ("AEOI") and Novin Energy Company.

612. In 2007, Bank Mellat was designated by the U.S. Treasury Department for providing "banking services in support of Iran's nuclear entities, namely the Atomic Energy Organization of Iran (AEOI) and Novin Energy Company. Both AEOI and Novin Energy have been designated by the United States under E.O. 13382 and by the UN Security Council under UNSCRs 1737 and 1747."

613. During the relevant time period, Bank Mellat provided financial services and maintained Eurodollar accounts for AEOI and Novin Energy Company, and as part of the Conspiracy, Bank Mellat affirmatively worked to prevent disclosure of its dollar-denominated transactions on behalf of these designated customers.

614. In June 2006, Bank Mellat was involved in a transfer totaling over $250 million dollars into a Eurodollar account it held for Novin Energy Company.

615. As part of the Conspiracy, the CBI effectuated the payment(s) in USD funds to Bank Mellat's Eurodollar account in London for further credit to the Eurodollar account of Bank Mellat's client – Novin Energy Company.

616. In 2007, Bank Sepah facilitated payments in USD funds to Eurodollar accounts at Bank Mellat on behalf of entities associated with Iran's Aerospace Industries Organization ("AIO"), a subsidiary of Iran's Ministry of Defense and Armed Forces Logistics ("MODAFL")

that was designated by the United States on June 28, 2005.[35]

617. The AIO is the Iranian organization responsible for ballistic missile research, development and production activities and organizations, including the Shahid Hemmat Industries Group ("SHIG") and the Shahid Bakeri Industries Group ("SBIG"), which were both listed under U.N. Security Council Resolution 1737 and designated by the United States under E.O. 13382.

618. Bank Mellat was designated by the United States on October 25, 2007 in connection with Weapons of Mass Destruction proliferation activities and was included on OFAC's SDN list. The designation, *inter alia*, excluded Bank Mellat from accessing the U-Turn exemption for Iranian Eurodollar transactions.

619. In 2002, together with Iran's Bank Tejarat, Bank Mellat merged its London branch to form Persia International Bank Plc in the United Kingdom.

620. During the relevant time period, both Defendant HSBC-London and Defendant Barclays maintained Eurodollar accounts for Persia International Bank Plc and served as its "principal bankers" in the Eurodollar market.

G. BANK SEPAH'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

621. Bank Sepah is an Iranian government-owned and government-controlled financial institution.

622. In 2007, the U.S. Treasury Department designated Bank Sepah for providing support and services to designated Iranian proliferation firms. The designation was effectuated

[35] When Bank Sepah was designated by the U.S. in January 2007, the U.S. government noted that "Bank Sepah is AIO's bank of choice, and since at least 2000, Sepah has provided a variety of critical financial services to Iran's missile industry, arranging financing and processing dozens of multi-million dollar transactions for AIO and its subordinates…" *See* https://www.treasury.gov/press-center/press-releases/Pages/hp219.aspx.

pursuant to E.O. 13382, due to Bank Sepah's Weapons of Mass Destruction proliferation-related activities.

623. Bank Sepah International Plc, a wholly owned subsidiary of Bank Sepah in the United Kingdom, was also designated.

624. According to the U.S. Treasury Department, Bank Sepah was the financial linchpin of Iran's missile procurement network and actively assisted Iran's pursuit of missiles capable of carrying Weapons of Mass Destruction.

625. As a result of the designation, Bank Sepah (including Bank Sepah International Plc) was excluded from accessing the U-Turn exemption for Eurodollar transactions.

626. During the relevant time period, Defendant HSBC-London provided illegal Eurodollar clearing and settlement services to Bank Sepah.

627. During the relevant time period, Standard Chartered Bank provided illegal Eurodollar clearing and settlement services for Bank Sepah, as well as facilitating US dollar-denominated Letters of Credit for Bank Sepah. SCB, as discussed *infra*, also provided Eurodollar payments and trade-finance services for Bank Saderat and Bank Melli.

628. As detailed below, Bank Sepah, acting in concert with SCB, illegally financed the acquisition of U.S. goods on behalf of Mahan Air.

629. For example, in February 2006, Credit Suisse in Zurich paid SCB Dubai almost $30 million dollars (cleared and settled through the United States) on behalf of Bank Sepah, which had, in turn, financed Mahan Air's acquisition of an Airbus A320-232 and several aircraft engines.[36]

[36] Part of the trade-finance transaction was cleared through Standard Chartered's New York branch, and the paperwork indicates that SCB was aware that the transaction involved U.S. origin parts prohibited by U.S. sanctions.

630. In another case in 2002, Bank Sepah financed (in USD funds) the purchase of U.S. aircraft parts from an Iranian front company—the Malaysian and UK exporter Downtown Trading Ltd—on behalf of a MODAFL-controlled entity.

631. As part of the illegal scheme, once the U.S.-manufactured goods were transported from Malaysia to Iran by Iran Air, Downtown Trading Ltd., Malaysia sent documents to its bank, Maybank, Malaysia to collect payment against the Letter of Credit.

632. Maybank then presented documents under Bank Sepah's Letter of Credit to SCB, Dubai (the Negotiating Bank) for validation and subsequent clearing and settlement of the transaction's final Eurodollar payment through Citibank, New York.

633. Thus, Bank Sepah, with the assistance of Maybank and SCB, financed the illegal acquisition of U.S. aircraft parts by MODAFL, and induced Citibank in New York to provide dollar clearing and settlement to consummate the transaction.

634. As detailed below, Defendant Commerzbank AG's New York branch also provided illegal Eurodollar clearing and settlement services for Bank Sepah.

H. JOHN DOE DEFENDANTS' 1-50 AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

635. Other non-defendant co-conspirators (including other Iranian financial institutions and entities) conspired with the named Defendants and identified non-defendant Co-conspirators herein. Plaintiffs may amend this Complaint to identify such other non-Defendant Co-conspirators as additional evidence warrants.

636. The true names, residences and capacities, whether individual, corporate or otherwise, of Defendants John Does 1 through 50 (collectively, the "Does") are presently unknown to Plaintiffs, who therefore sue those Defendants under such fictitious names. The Does are other financial institutions, their agents, officers and/or employees that conspired with the Western Bank

Defendants, Iran, and the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc). Each of the Does is responsible in some manner for the acts alleged herein and for the damages that each Plaintiff sustained. As warranted by the evidence, Plaintiffs will amend this Complaint to show the true names and capacities of the Does when they are ascertained and confirmed.

I. THE HSBC DEFENDANTS' AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

637. The HSBC Defendants have a longstanding relationship with Iran.

638. In 1999, HSBC Group established a relationship with the Tehran office of Bank Melli Iran, and it launched an "Iran Representative" office in Tehran, Iran that same year.

639. In December 2000, HSBC Group members entered into a $500 million project finance agreement with six Iranian commercial banks: Bank Saderat Iran, Bank Melli Iran, Bank Mellat, Bank Tejarat, Bank Sepah and the Export Development Bank of Iran ("EDBI").

640. Beginning in the late 1990s, Defendant HBSC-Europe and Defendant HSBC-Middle East devised a procedure whereby their Iranian Bank Co-conspirators put a cautionary note in their SWIFT-NET payment order messages including language such as, "*care sanctioned country,*" "*do not mention our name in NY*," and "*do not mention Iran.*"

641. Eurodollar payment transactions with these cautionary notes automatically fell into what Defendant HSBC-Europe termed a "repair queue," where employees of HBSC-Europe and HSBC-Middle East manually removed all references to Iranian-sanctioned entities from the SWIFT-NET messages associated with each transaction.

642. Between 2001 and 2007, the HSBC Defendants actively participated in the Conspiracy by repeatedly undertaking various methods to facilitate Eurodollar payments, trade finance and foreign exchange transactions on behalf of Iran through the United States that would

evade U.S. sanctions by disguising Iran's financial activities as its USD funds were cleared and settled by U.S. financial institutions, including Defendant HSBC-US.

643. Unlawful Iranian transfers of USD funds from HSBC-Europe and HSBC-Middle East were sent through the HSBC Group's USD correspondent accounts at HSBC-US by:

a. Deleting references to Iran from the payment instructions (a.k.a. "stripping" the transactions), or otherwise altering the SWIFT-NET messages, to either omit or falsify information that would have otherwise indicated Iran's involvement in the transaction; and

b. Styling transactions as bank-to-bank "cover" transactions between two non-Iranian banks, solely because the MT 202 payment order message format used for such transactions did not expressly obligate HSBC to identify the transaction's originator and beneficiary, thus avoiding any disclosure of the transaction's Iranian connections, and blocking HSBC-US's electronic filter algorithms from recognizing the transaction, let alone assessing whether it qualified for any OFAC exemption or license.

644. Defendant HSBC-Europe created detailed plans to avoid triggering HSBC-US's automated OFAC filter software and reduce the need for "manual intervention" (*e.g.* the re-formatting Eurodollar transactions), thus sparing HSBC-Europe's employees from the need to manually alter the SWIFT-NET messages in order to remove references that might otherwise identify the presence of Iranian parties to the transaction, and associated scrutiny.

645. This enabled the HSBC Defendants' business with Iran in the Eurodollar market to proceed quickly and profitably.

646. In 2010, facing U.S. government investigations, HSBC-US hired Deloitte LLP as its outside auditor to identify and examine HSBC Group's OFAC sensitive USD funds transactions involving Iran and other prohibited countries or persons that went through the bank.

647. That "review" identified more than 25,000 illegal transactions that involved Iran, worth a total of more than $19.4 billion in USD funds.

648. The payment orders had been sent to HSBC-US and other financial institutions in the United States without referencing Iran, ensuring that the Eurodollar payment transactions would be processed without delay and not be blocked nor rejected by the algorithms in the automated OFAC filtering systems.

649. The HSBC Defendants deliberately amended SWIFT-NET payment order messages and used MT 202 cover payments to conceal the nature of the transactions from HSBC-US automated OFAC sanction screening filters and those of other financial institutions in the United States, and HSBC-US was aware that the other HSBC Defendants used such methods to alter payment order messages.

650. At the same time, the HSBC Defendants further trained, mentored and educated their Iranian Co-conspirators on how to deceptively format SWIFT-NET payment order messages, *inter alia*, to avoid detection and scrutiny by U.S. financial institutions, thus ensuring that Iran could solicit other conspirators to facilitate Eurodollar payments in a like manner.

651. Accordingly, the HSBC Defendants' (and other Defendants' and Co-conspirators') willingness to process payments in this manner enabled Iran to flood the global financial system with undetectable U.S. dollar payment transactions and effectuate—what would have otherwise been preventable—transfers of USD funds to Hezbollah and the IRGC.

652. Defendant HSBC Holdings was aware of Defendants HBSC-Europe and HSBC-Middle East's involvement in the Conspiracy with Iran as early as 2000.

653. For example, HSBC Group AML Compliance Head Susan Wright received an email on June 9, 2000, from Bob Cooper, an HSBC colleague, informing Wright of an existing procedure that the HSBC Defendants were already employing to avoid OFAC filter detection.

654. Cooper explained:

a. A client bank had been "*automatically replacing a remitter's name with that of*" the client bank and that bank was utilizing bank-to-bank "cover payments" because the payment message formats did not expressly require identification of either the underlying party originating the transaction or the transaction's ultimate beneficiary.

b. In the future, for OFAC sensitive transactions, that bank would "*arrange cover for the payment using MT202/203 remittances*."

c. In addition, that bank planned to send a separate 'MT100 message' to the recipient bank, providing full payment details for the originator and ultimate beneficiary.

655. Cooper's email overtly acknowledged that "[i]n this way a payment in US$ can be made for an individual or company on the OFAC list, without the name being 'detected' by the OFAC filters that all US banks would apply."

656. Several days later, on June 14, 2000, Wright forwarded Cooper's June 9, 2000 email to the then-current Head of HSBC Group Compliance, Matthew King.

657. In her cover email, Wright stated that the "practice" detailed by Cooper was "unacceptable" and informed King that it was her position that:

a. "We advised them that this was contrary to SWIFT guidelines (drawn up to address FATF concerns re money laundering via wire transfers) which required that the full details (names and addresses) of remitters and beneficiaries are included."

b. "From a Group perspective I consider the continuation of this practice [the client bank's future plan to conceal OFAC sensitive transactions behind bank-to-bank transfers] to be unacceptable as a deliberate and calculated method to avoid US OFAC sanctions and has the potential to raise serious regulatory concerns and embarrass the Group."

658. Senior HSBC Group officials were aware of the Conspiracy, including the specific methods and overt acts by which Iran, the Iranian banks and the HSBC Defendants were carrying it out.

659. However, despite this awareness, senior compliance officials of HSBC Group and its subsidiary banks and entities (including compliance officials at Defendants HSBC Holdings, HSBC-Europe, HSBC-Middle East, and HSBC-US) did *not* put an end to this illicit banking "practice" with Iran. Instead, with clear knowledge of its purpose—and awareness that other banks participated in the Conspiracy—they knowingly employed similar techniques to evade OFAC requirements, thus allowing the HSBC Defendants to continue deploying and refining their respective "procedures" to facilitate illegal Eurodollar payments from and for Iran in USD funds.

660. In late 2000, in coordination with the CBI, HSBC signed a project finance framework agreement with six Iranian commercial banks: Bank Melli, Bank Saderat, Bank Mellat, Bank Tejarat, Bank Sepah and the Export Development Bank of Iran.

1. HSBC-Europe's 2001 "Bank Melli Proposal"

661. In or around January 2001, Bank Melli's London branch maintained Eurodollar accounts with several other major international banks but was interested in establishing a relationship with HSBC that would give HSBC the majority of Bank Melli's USD funds clearing and settlement business.

662. In an April 30, 2001 letter, Defendant HSBC-Europe presented Bank Melli in London with a proposal (the "Bank Melli Proposal") for processing Bank Melli payments. HSBC-Europe's proposal boasted that HSBC-Europe was "…confident that we have found a solution to processing your payments with minimal manual intervention."

663. The Bank Melli Iran Proposal expressly underscored that, if it adopted HSBC-Europe's "solution," Bank Melli would not be identified as a sender in any payment order message and, thus, HSBC-Europe would ensure that Iranian transactions involving USD funds would not run into any 'speed bumps' or other obstacles.

664. The "solution" provided specific alternative wording, as it explained:

> "The key is to **always** populate field 52 – if you do not have an ordering party then quote 'One of our Clients,' **never leave blank.** This means that the outgoing payment instruction from HSBC will not quote 'Bank Melli' as sender – just HSBC London and whatever is in field 52. This then negates the need to quote 'DO NOT MENTION OUR NAME IN NEW YORK' in field 72." [Emphasis in original.]

665. HSBC-Europe's proposal further requested, "In order to test our proposed solution we would appreciate if you used the following templates when submitting your next payments to the following customer, or alternatively submit a USD 1 test payment" and provided the following:

> **MT202**
> 20: *Your Ref….*
> 21: *Related Ref….*
> 32: *Amount/currency/Value date….*
> 50: **DO NOT QUOTE IF IRANIAN**
> 52: *Customer Name* **OR** *One of our clients* **MUST BE COMPLETED**
> 53: **/68296908**
> 54:
> 56:
> 57: *Beneficiary Banker (SWIFT codes where possible)*
> 58: *Beneficiary (SWIFT codes where possible)*
> 70: *Any Payments details for beneficiary…*
> 72: **Please leave blank**
> **MT100**
> Pay as above.
>
> (Emphasis in the original.)

666. Thus, the Bank Melli Proposal documented the HSBC Defendants' active coordination and participation in the Conspiracy to illegally remove, omit or falsify essential information from SWIFT-NET messages so as not to trigger OFAC sanctions screening filters or otherwise permit HSBC-US or other U.S depository institutions to detect Iranian transactions in USD funds.[37]

[37] An internal HSBC memorandum that was associated with the Bank Melli Proposal also makes clear HSBC's awareness of Defendant Standard Chartered Bank's role as NIOC's primary (Western) banker at the time.

667. In 2001, John Wilkinson served as HSBC-Europe's Institutional Banking Relationship Manager for HSBC-Europe's Bank Melli account.

668. In a June 28, 2001 email titled "**Re: Bank Melli**" to HSBC-US, Wilkinson discussed the Bank Melli Proposal, describing HSBC-Europe's "usual method" to alter the wording of Iranian payment order messages, and the rationale for doing so:

- "Once the proposition goes live, we have instructed Bank Melli to alter the format of its [sic] payments to achieve straight through processing. The field 52 input of 'one of our clients' is a standard phrase used by MPD [Multicurrency Payments Department] in these situations."

- "Since sending the letter we have further asked them to only put 'One of our clients' in field 52, thus removing the chance of them inputting an 'Iranian referenced' customer name, that causes fall out of the cover payment sent to HSBC-US and a breach of OFAC regulations."

669. In further support of his position to continue this standard 'procedure,' Wilkinson explained that a payment involving an Iranian bank had been blocked because HSBC-Europe's MPD [Multicurrency Payments Department] "failed to spot the poor input and did not follow the normal procedure of altering the payment."

670. In other words, the HSBC Defendants' "normal" procedure was to conspire with Iranian banks, including Bank Melli, to *deliberately* alter payment order messages prior to sending them to New York for the express purpose of avoiding detection and analysis by U.S. banks, regulators and law enforcement.

671. In an email exchange in October 2001 between David Bagley, Defendant HSBC-Middle East's Regional Head of Legal and Compliance, and Matthew King, a member (and later Head of) HSBC Group's Audit Department, King noted:

> We also have to bear in mind pending US legislation which will in effect give the US extraterritorial authority over foreign banks, particularly if we are unfortunate enough to process a payment which turns out to be connected to terrorism. My own view therefore is that some of the routes

> traditionally used to avoid the impact of US OFAC sanctions may no longer be acceptable.

672. HSBC Group AML Head Susan Wright and Money Laundering Control Officer John Allison received copies of King's e-mail.

673. King's email further confirms that senior executives and managers within the HSBC Group comprehended what the HSBC Defendants (and other foreign banks) had "traditionally" been doing for years when they used "routes" (a euphemism for altering payment order messages prior to routing them to U.S. financial institutions through SWIFT-NET) to avoid disclosing a transaction's Iranian connections, and that some of those transactions might prove to be "connected to terrorism."

674. A January 2003 memorandum authored by HSBC-Middle East and disseminated to other members of the HSBC Defendants confirms not only the HSBC Defendants' ongoing participation in the Conspiracy, but also their knowledge of the participation of other co-conspirators, and Iran's desire to further evade U.S. sanctions.

675. The memorandum stated in relevant part:

- "It is believed that some service providers amend the payments to ensure Iran is not mentioned in the body of the payment instruction to their USD correspondent. This process minimizes the risk of payment being referred to OFAC."

- "Currently, it is estimated that Iranian banks issue up to 700 USD payments a day using their USD providers, mainly banks in the UK and Europe, which in turn use their New York USD correspondents to effect the payments."

676. In addition to acknowledging the existence of the Conspiracy, the HSBC-Middle East memorandum also advised:

> "[T]here is substantial income opportunity to sell a USD payments proposition to Iranian banks in view of the impending FATF regulations...The [requirements of the] new regulations…increases the risk

> of Iranian payments being held in the USA as they may fall foul of the OFAC regulations. The Iranian Banks have now prioritized this issue and are now actively seeking a solution from their banks, including HSBC."

677. From at least 2003 forward, HSBC provided banking and payment services in the Eurodollar market to, among other Iranian entities, the NIOC (which, as noted previously, was later designated pursuant to E.O. 13382 and identified as an agent or affiliate of the IRGC during the relevant time period).[38]

678. Over the course of the next several years, the HSBC Defendants continued their participation in the Conspiracy.

679. In an October 9, 2006 email, David Bagley [HSBC-Middle East's Regional Head of Legal and Compliance] informed senior HSBC Group officials that key U.S. policymakers were "…in favour of withdrawing the U-Turn exemption from all Iranian banks. This on the basis that, whilst having direct evidence against Bank Saderat particularly in relation to the alleged funding of Hezbollah, they suspected all major Iranian State-owned banks of involvement in terrorist funding and WMD [weapons of mass destruction] procurement."

680. Further demonstrating his awareness of the risks HSBC was engaged in with Iran, Bagley was listed as the contact person on the April 19, 2007 Wolfsberg Group press release calling for more transparency for international wire transfers "to promote the effectiveness of global anti-money laundering and anti-terrorist financing programs."

---

[38] The HSBC Defendants also provided Eurodollar, trade-finance, and foreign exchange services for NIOC. For example, the aforementioned January 2003 HSBC-Middle East memorandum stated that:

> L/C's [Letters of Credit] issued for Iranian Companies Abroad – Various Group Offices. HSBC offices are developing relationships with Iranian Government and non-Government companies. The L/C's issued are normally denominated in USD. Following NIOC's acceptance of HSBC as one of its listed banks, HSBC Bank Middle East now handles Iran's oil export L/C's. Turnover for this business is about USD400M [million] per year.

681. Eight months later, in a June 8, 2007 email, Bagley informed HSBC Holding's CEO, Michael Geoghegan, and others, that "[U.S. Treasury Under Secretary for Counter Terrorist Financing and Sanctions] Levey essentially threatened that if HSBC did not withdraw from relationships with [redacted] we may well make ourselves a target for action in the US."

682. Bagley's email thus confirmed that various relationships continued to exist in the Eurodollar market with Iran and Iranian banks, including Bank Saderat.

683. Bagley not only acknowledged that HSBC had "…an agency banking relationship in HSBC-EUROPE both for [redacted] and other Iranian banks," but he confessed that "[t]here are further complications surrounding the process of closure with all Iranian banks as we have some USD 9m in reimbursements due from Sepah, where we are running off trade lines, where we may need cooperation from Central Bank of Iran."

684. On December 11, 2012, the U.S. Department of Justice ("DOJ") announced that Defendants HSBC Holdings and HSBC-US had admitted to Anti-Money Laundering ("AML") and OFAC sanctions violations, and had agreed to enter into a Deferred Prosecution Agreement and pay a $1.256 billion forfeiture. As explained further *infra*, DOJ issued a press release announcing the DPA, and summarizing the HSBC Defendants' illegal conduct.

685. In connection with the DPA, DOJ filed a four-count felony criminal information against HSBC Holdings and HSBC-US, charging them with: (1) willfully failing to maintain an effective AML program; (2) willfully failing to conduct due diligence on their foreign correspondent affiliates; (3) violating the International Emergency Economic Powers Act ("IEEPA"); and (4) violating the Trading with the Enemy Act ("TWEA"). HSBC Holdings and HSBC-US waived federal indictment, agreed to the filing of the information, and claimed to have accepted responsibility for HSBC's and its employees' criminal conduct.

686. Despite its agreement to overhaul its U.S. and global compliance functions, HSBC remained a conduit for illicit funds.

687. On December 9, 2010, the U.S. Treasury Department designated Tajco, describing it as "a multipurpose, multinational business venture involved in international trade as well as real estate and presided over by Ali Husayn and Kassim Tajideen…. Since at least December 2007, Ali Tajideen used Tajco Sarl, operating as Tajco Company LLC, as the primary entity to purchase and develop properties in Lebanon on behalf of Hizballah."

688. The designation also covered Kairaba Supermarket, a subsidiary business of Tajco Ltd.

689. A July 13, 2012 article published by *Reuters* entitled "Special Report: HSBC's Money-Laundering Crackdown Riddled With Lapses" reported that an HSBC-US compliance officer had identified suspicious transactions involving Hezbollah, specifically Tajco and Kairaba Supermarket.

690. In December 2013, the Treasury Department announced that Defendant HSBC-US agreed to remit $32,400 to settle potential civil liability for three apparent violations of the Global Terrorism Sanctions Regulations, 31 C.F.R. Part 594.

691. The fine reflected the fact that HSBC-US facilitated transactions in late 2010 and early 2011 worth about $40,000 that benefited Tajco.

692. Although a relatively small sum, the facilitation of terrorism financing for Hezbollah a considerable time after Defendants HSBC Holdings and HSBC-US began negotiating their deal with DOJ, strongly suggests that, as of early 2011, the HSBC Defendants had not seriously remediated their AML/CFT controls and procedures, even after being caught committing hundreds of felonies.

2. Defendant HSBC-US's Agreement to, and Participation in, the Conspiracy in Violation of 18 U.S.C. § 2332d

693. As alleged in greater detail below, even though at all relevant times Defendant HSBC-US was aware that: the HSBC Defendants were participating in the Conspiracy to unlawfully transmit Iranian USD funds through U.S. banks (including HSBC-US); and periodically complained about Defendants HSBC-Middle East and HSBC-London's conduct and proposed new procedures and policies for HSBC Group members that would have provided HSBC-US improved transparency, HSBC-US took no measures to prevent HSBC-US from facilitating hundreds of millions of dollars of payments to Iran in violation of 18 U.S.C. § 2332d. Accordingly, in addition to violating § 2332d, HSBC-US's conduct evidenced its agreement to continue participating in the Conspiracy despite its complaints, its knowledge or deliberate indifference to the Conspiracy's criminal objectives and purposes, and its commission of multiple overt acts in furtherance of the Conspiracy.

694. One key example of HSBC-US's failure to take substantive measures to ensure that it would not facilitate the HSBC Defendants' provision of illegal material support and services to Iran is reflected in a July 12, 2001 e-mail to senior employees at HSBC-US (containing a memorandum authored by HSBC Group Representative for Iran, John Richards).

695. Richards's memorandum outlined the business opportunities members of the HSBC Group were presented with in connection with prospects to expand and grow HSBC Group's relationships with Iran, the CBI and Bank Melli, explaining:

a. "We have been approached by the Central Bank of Iran to take back their USD clearing business from Natwest. In principal I am keen to do this but on the clear proviso that it can be done profitably and on a sustainable basis."

b. "One of our key objectives for the year is to develop HSBC's Asset Management activities in Iran and with the Central Bank now

> managing the oil price stabilization fund amounting to some USD10bn there is considerable scope for this. Obviously many foreign banks are chasing the same business and so we need to demonstrate some competitive or relational advantage. The proposal from the Central Bank was therefore not unwelcome…The Central Bank manages their transactions through Bank Melli London…"

c. "In summary if we can make this business independently profitable and sustainable the benefits that we can derive particularly from the Treasury Asset Management and Investment spin offs will be substantial."

696. Richards's memorandum also demonstrates the HSBC Defendants' awareness that other foreign banks (including Defendants) were eagerly pursuing U.S. dollar clearing and settlement business with the CBI in the Eurodollar market.

697. On July 12, 2001, Denise Reilly, HSBC-US's Senior Manager in Payment Operations, sent an e-mail titled "Re: Bank Melli" to various senior HSBC-US employees in which she stated, "It was relayed to us that the Group (with the Backing of Bond) [the Chairman] was looking to significantly grow our presence in Iran." Reilly also explained that the "current lines of credit [for Iran] were reported to be $800m, trade lines of $150m and growth was anticipated in trade, cash management and internet banking."

698. Thus, HSBC-US senior employees understood the significance to the HSBC Defendants of their Iranian business and specifically, the HSBC Defendants' relationship with Bank Melli.

699. As early as 2001, senior HSBC-US payments, compliance and business managers were informed that Iranian Eurodollar payment transactions were being sent by Defendant HSBC-London to HSBC-US for clearing and settlement in USD funds after references to Iran had been deleted.

700. HSBC-US employees were also informed of an HSBC-London proposal to streamline the processing of Iranian U-turn transactions by omitting references to Iran so that the payment orders would not be halted by OFAC's sanctions screening filter in the United States. Emails at the time show that senior HSBC-US officials expressed discomfort with the HSBC-London proposal, but took no other action to stop or prevent the activity already occurring.

701. As noted above, a senior HSBC-US employee received an e-mail on June 28, 2001 titled "*Re: Bank Melli*," which described HSBC-London's "usual method" of altering payment order messages and the reasons for doing so.

702. Another example of HSBC-US' knowledge and acquiescence in the Conspiracy is memorialized in a November 14, 2002 memorandum entitled "COMPLIANCE-OFAC ISSUES IN GENERAL AND SPECIFIC TO IRAN" authored by HSBC-London's Multicurrency Payments Department Head Malcolm Eastwood ("the Eastwood Memorandum").

703. The Eastwood Memorandum was sent to both HSBC-US and HSBC-London employees and forwarded to additional HSBC-US employees in separate emails.

704. The Eastwood Memorandum discussed both HSBC's "cover payment method" of evading U.S. sanctions and the specific actions taken by HSBC to modify the contents of payment messages. In relevant parts, the Eastwood Memorandum stated:

- "As the custodian of HSBC-Europe's payments operation I currently feel that we may be exposing ourselves to unnecessary and unacceptable Reputational and Operational Risk when we are handling payments originating from FIs [financial institutions] domiciled in or who are a local branch of an FI domiciled in an OFAC regulated country."

- "HSBC-Europe's historical practice has been to send these types of payments where the U Turn principal applies (ie funds are generally moving from an European bank to another European bank for the credit of an OFAC regulated entity) via the Cover Payment method. This means that the payment instructions received by HSBC-US

> contains no mention of the country or entity involved. My understanding is that this has been accepted practice for many years and that HSBC-Europe IBL hold accounts, some in USD for FIs domiciled in these countries ie Cuban, Iranian etc."

- "The Iranian banks continue to send us what I describe as conditional payment instructions which for HSBC-Europe require an element of amendment by ourselves. This introduces operational risk and under FATF principles we should not be amending these payments instructions. Acceptance of these items over many years means that we are bound by the precedents currently in place, and I believe that we need to break these precedents…"

- "[W]e need…[t]o agree a 'template' payment instruction for these U Turn Payments which can be used by PCM Sales and the RM team and sent to the Iranian Banks stipulating that payments must be formatted in this way, confirming that we will be sending these via the Serial method and that any deviation from this template will be at the Iranian Banks own risk."

- "Whilst I am told that there are significant business opportunities particularly with countries such as Iran there are also substantial Reputational and Operational Risks, not to mention financial losses associated with it."

705. In addition, HSBC-US's OFAC filter occasionally stopped an Iranian-related transaction, sent by an HSBC Group affiliate, in which the identifying information had inadvertently been retained, demonstrating that undisclosed Iranian U-Turn exemption transactions continued to be sent through HSBC-US correspondent accounts.

706. HSBC-US employees were copied on similar memoranda issued by other HSBC Defendants during the relevant period. For example, a January 2003 memorandum circulated by HSBC-Middle East (and received by several HSBC-US employees) also noted that "[t]he Group now has an excellent relationship with all Iranian banks and some very larger Iranian corporates such as National Iranian Oil Co, National Petrochemical Co, National Iranian Gas Co, National Iranian Steel Co, top Iranian insurance companies, Ministry of Power, Ministry of Post and Telecommunications, etc."

707. The memorandum also confirmed the HSBC Defendants' awareness that other non-Iranian banks were participating in the Conspiracy, stating:

- "It is believed that some service providers amend the payments to ensure Iran is not mentioned in the body of the payment instruction to their USD correspondent. This process minimizes the risk of payment being referred to OFAC."

- "Currently, it is estimated that Iranian banks issue up to 700 USD payments a day using their USD providers, mainly banks in the UK and Europe, which in turn use their New York USD correspondents to effect the payments."

- "[T]here is substantial income opportunity to sell a USD payments proposition to Iranian banks in view of the impending FATF regulations...The [requirements of the] new regulations…increases the risk of Iranian payments being held in the USA as they may fall foul of the OFAC regulations. The Iranian Banks have now prioritized this issue and are now actively seeking a solution from their banks, including HSBC."

708. An October 2003 document entitled "IRAN-STRATEGY DISCUSSION PAPER" circulated to senior HSBC-US employees further documented the HSBC Defendants' eagerness to facilitate USD funds transfers for Iran, noting: "One of the reasons to accelerate our process of engagement is to demonstrate, to the authorities within Iran, that we are committed to the development of their country. This is seen to be particularly important given the more aggressive/pragmatic approach to Iranian business adopted by French and German competitor banks."

709. Nevertheless, despite being copied on such memos, HSBC-US took no further action to stop the unlawful activities.

710. Even when HSBC-US blocked Iranian payment transactions, it failed to take further action to ensure that other HSBC Defendants would not continue these illegal practices.

711. For example, in late December 2002, HSBC-US's OFAC sanctions screening filter stopped and rejected a payment order listing Bank Melli as the originator of the SWIFT-NET message that contained a field that read, "**Do not mention our name in NY**."

712. An internal HSBC-US email dated December 30, 2002, informed HSBC-US's compliance team about the Bank Melli payment, which once again confirmed the HSBC Defendants' ongoing process of altering payment order messages.

713. On June 13, 2003, HSBC-US's OFAC filter stopped another transaction, this time for $150,000 in USD funds, because it included both a reference to Bank Melli and the words "*do not mention our name.*"

714. In a June 16, 2003 email entitled "PLC-Re do not mention our name," HSBC-US compliance officers were notified about the June 13 blocked transaction and received additional confirmation of the HSBC Defendants' illegal practice of altering fields within Iranian payment order messages for the express purpose of escaping detection in the United States.

715. During 2004, in furtherance of the Conspiracy, HSBC Group members sent approximately *7,000* Iranian Eurodollar transactions through various SWIFT-NET network accounts for clearance and settlement by Defendant HSBC-US and other correspondent banks in the United States without disclosing their source.

716. HSBC-US did not report any of the HSBC Defendants' illegal conduct involving Iran to any of its regulators or to U.S. law enforcement at that time.

717. During 2005, in furtherance of the Conspiracy, HSBC-London and HSBC-Middle East together sent about *5,700* Iranian Eurodollar transactions through various SWIFT-NET network accounts for clearance and settlement by Defendant HSBC-US and other correspondent banks in the United States without disclosing their source.

718. On April 19, 2005, HSBC-US's OFAC filter again stopped a $362,000 payment order from Bank Melli because it contained the phrase "*do not mention our name in New York.*"

719. HSBC-London re-submitted the same payment on April 22, 2005, but HSBC-US stopped it again, this time sending HSBC-London a SWIFT-NET message requesting full disclosure of the name and address of the underlying originator and ultimate beneficiary of the USD funds.

720. In early May 2005, HSBC-US stopped a $6.9 million USD payment order originating with Defendant Credit Suisse in Zurich because the SWIFT-NET message details included the phrase "*Bank Melli Iran*."

721. In fact, forty-four of the payments stopped by HSBC-US's OFAC filter in May 2005 alone (inadvertently) disclosed Iranian involvement.

722. On June 3, 2005, HSBC-US informed Defendant HSBC Holdings that additional HSBC-London transfers in the amounts of $1.9 million USD and $160,000 USD had been stopped by HSBC-US due to the lack of full disclosure of the originator, beneficiary, and purpose of the payment transaction.

723. HSBC-London responded that both payment orders were foreign exchange related, the originators were Bank Tejarat and Bank Melli,[39] and the beneficiaries of the USD funds were Persia International Bank and Defendant Credit Suisse's Zurich office, respectively.

724. HSBC-US responded by requesting that HSBC-London follow up with the banks to obtain the names and addresses of the initial originators and ultimate beneficiaries, as well as confirmation of the underlying purpose of the payments.

[39] HSBC-London also maintained correspondent accounts for Bank Refah.

725. According to information provided by Bank Melli through HSBC-London, the $160,000 payment denoted an internal transfer from Bank Melli's Eurodollar account with HSBC-London to Bank Melli's Eurodollar account with Defendant Credit Suisse's Zurich office.

726. From July 2005 to June 2006, HSBC-Middle East sent more than 2,500 Iranian Eurodollar transactions – through its various SWIFT-NET network accounts for clearance and settlement by Defendant HSBC-US and/or other correspondent banks in the United States – that illegally concealed the required data relating to Iran.

727. On November 23, 2005, in an email entitled "Cover payment processed to Credit Suisse re 'Bank Melli' – USD 100,000," an HSBC-US OFAC Compliance officer notified HSBC-London that, on November 7, 2005, a $100,000 transaction involving Bank Melli had been processed through HSBC-London's USD account at HSBC-US without transparent documentation:

> We are bringing this to your attention as this situation indicates that cover payment involving Iran are still being processed by PLC [referring to HSBC-London]. It was our understanding that Group payments involving Iran would be fully disclosed as to the originators and beneficiaries.

728. In furtherance of the Conspiracy, from April 2006 through December 2007, about 50% of the estimated *700* Iranian Eurodollar payment transactions sent by HSBC-London – through its various SWIFT-NET network accounts for clearance and settlement by Defendant HSBC-US and/or other correspondent banks in the United States – continued to not disclose their connection to Iran.

729. In addition, through March 2010, HSBC-US was the conduit for at least twenty-four post-U.S. designation Eurodollar transactions on behalf of IRISL and/or its various subsidiaries and front companies.

730. During the relevant time period, HSBC-US knew that Iran was a designated State Sponsor of Terrorism, and that HSBC-US's USD clearing and settlement operations with CHIPS-NY (Eurodollar clearing and settlement), CLS Bank (foreign exchange) and FRB-NY (domestic USD clearing and settlement and central bank lender of last resort for the Eurodollar market) were being used by the HSBC Defendants to facilitate unlawful transactions in USD funds on behalf of Iran in furtherance of the Conspiracy.

731. As noted above, on December 11, 2012, Defendants HSBC Holdings and HSBC-US entered into a Deferred Prosecution Agreement with DOJ.

732. DOJ issued a press release announcing the 2012 DPA's entry, including the fact that the DPA resulted in HSBC Holdings and HSBC-US admitting to AML and sanctions violations, as well as the fact that they would pay a $1.256 billion USD forfeiture.

733. In addition to the $1.256 billion forfeiture under the DPA, HSBC Holdings and HSBC-US also agreed to pay $665 million in civil penalties – $500 million to the OCC and $165 million to the Federal Reserve – for the HSBC Defendants' AML/CFT program violations with Iran, other sanctioned countries, and transnational drug cartels.

734. DOJ's press release announcing the DPA quoted then-Assistant Attorney General Lanny Breuer:

> HSBC is being held accountable for stunning failures of oversight – and worse – that led the bank to permit narcotics traffickers and others to launder hundreds of millions of dollars through HSBC subsidiaries, and to facilitate hundreds of millions more in transactions with sanctioned countries. The record of dysfunction that prevailed at HSBC for many years was astonishing.

735. The United States Attorney for the Eastern District of New York Loretta Lynch was quoted as stating:

> HSBC's willful flouting of U.S. sanctions laws and regulations resulted in the processing of hundreds of millions of dollars in OFAC-prohibited transactions. Today's historic agreement, which imposes the largest penalty in any [Bank Secrecy Act] prosecution to date, makes it clear that all corporate citizens, no matter how large, must be held accountable for their actions.

736. Manhattan District Attorney Cyrus R. Vance Jr. was quoted in the same press release as stating:

> New York is a center of international finance, and those who use our banks as a vehicle for international crime will not be tolerated. … Sanctions enforcement is of vital importance to our national security and the integrity of our financial system. The fight against money laundering and terror financing requires global cooperation, and our joint investigations in this and other related cases highlight the importance of coordination in the enforcement of U.S. sanctions.

J. DEFENDANT BARCLAYS' AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

737. Until at least May 2008, Defendant Barclays maintained correspondent banking relationships with several of the Iranian Bank Co-conspirators, including Bank Saderat and Bank Melli.

738. Barclays is a member of SWIFT-Brussels and has historically used the SWIFT-NET system to transmit international payment messages from and for financial institutions around the world.

739. Barclays originally processed USD payment messages through numerous global locations.

740. Over time, Barclays consolidated its USD payment processing so that the payments were predominately processed at Barclays' Payment Processing Centre located in Poole, England ("Poole").

741. Barclays knowingly and willfully engaged in conduct that caused its New York branch and other financial institutions in the United States to process Eurodollar payment transactions in violation of U.S. sanctions.

742. As part of this effort to evade U.S. sanctions against Iran, Barclays:

a. Followed instructions from Iran and its agents not to mention their names in USD payment transaction messages sent to Barclays-New York and to other U.S. financial institutions for clearance and settlement in USD funds;

b. Routed transactions through an internal Barclays sundry account, thereby hiding the payment transactions' connection to Iranian entities;

c. Amended or reformatted SWIFT-NET payment order messages to remove information identifying Iranian entities involved in the transfer of USD funds; and

d. Re-sent Iranian entities' SWIFT-NET MT 103 payment order messages as cover payments to take advantage of the lack of transparency as to the ultimate originator/beneficiary that was achieved by using the MT 202 bank-to-bank cover payment message format.

743. Beginning in 1987, Bank Melli Iran instructed Barclays to process USD transactions in favor of Bank Melli's London branch by referencing only Bank Melli's Eurodollar account number at Midland Bank Plc and without referencing Bank Melli's name.

744. Bank Melli further instructed Barclays to send separate payment order instructions, which included full details about the Eurodollar payment transactions to Midland Bank Plc and Bank Melli's London Branch.

745. In response, Barclays memorialized Bank Melli's instructions for Eurodollar market transactions in a memorandum sent by its Head Office to Barclays' international offices, and, as early as the late 1990s, included them in Barclays' "List of Correspondents" ("LOC"),

which contained information related to Barclays' correspondent banking relationships and assisted Barclays' employees in effectuating international payment transactions involving USD funds.

746. Barclays' LOC contained instructions on how to process payments for both sanctioned and non-sanctioned banks with which Barclays had correspondent relationships.

747. Over time, the LOC grew to include instructions for payments related to several of Barclays' correspondent bank clients and included instructions to use cover payments (SWIFT-NET MT 202 payment order messages) when processing payments in USD funds for clearing and settlement in the United States, and omitting the names of U.S.-sanctions targets from the payment order messages so that U.S. financial institutions could not identify the sanctions nexus of the payments.

748. In a November 1987 Head Office Circular, Barclays distributed payment instructions received from an Iranian bank directing Barclays "to amend the procedures governing the transfer of U.S. Dollars for any purpose in favour of our London branch" and to route such payments "without mentioning the name of our bank."

749. The reason for, and effect of, these instructions was to disguise Iranian sanctioned entity payments from Barclays' correspondents in the United States so that such correspondents would unwittingly process the illegal payments.

750. Barclays' employees followed the instructions in the LOC when processing USD payments involving sanctioned Iranian banks, thereby ensuring that the name of the bank would not appear in any MT 202 cover payment messages sent to Barclays' New York branch for clearing and settlement through CHIPS-NY and FRB-NY. For example, with regard to USD payments sent on behalf of an Iranian bank, the LOC stated, "[t]he cover MT202 for the direct Payment Order to

be arranged by the remitting Bank without mentioning [the Iranian bank's] name ...." (Underlined in the original.)

751. Barclays' LOC also contained instructions to contact the remitter or beneficiary for routing instructions for certain payments of USD funds involving Iranian sanctioned entities. The general instructions for Iranian banks stated:

> USD PAYMENTS TO IRAN
> Certain payments may be blocked by the US Authorities. Therefore, any branch with a USD transfer is advised to contact the remitter beneficiary or beneficiary's bankers to request specific routing instructions.

752. Barclays' standard operating procedures allowed and even educated its employees on how to bypass the sanction screening algorithms in both Poole's and the U.S. financial institution's OFAC filters to permit illegal payment transactions in USD funds.

753. Pursuant to these "standard" procedures, when the Poole filter identified a Eurodollar payment transaction that referenced an Iranian entity, that payment order message was stopped for further review by Barclays' employees in Poole.

754. If the Poole-based employees found that the payment order message referenced an Iranian entity, they would follow one of the following procedures: (i) return the payment order message to the remitting entity via a pre-formatted fax cover sheet; (ii) alter or delete fields in the SWIFT-NET payment order message; or (iii) change the message type from a serial payment (MT 103) to a cover payment (MT 202) in order to hide any connection to the Iranian entity.

755. The then-Senior Manager for Barclays Group Payments Industry Management in Poole explained that if the MT 202 payment order message contained beneficiary information that caused it to be stopped by the OFAC filter in the U.K., that information was removed to ensure the payment transaction was not stopped by the OFAC filter when resubmitted.

756. The same Senior Manager noted that he was aware that Defendant Barclays' payment operators amended payment order messages in order to facilitate the transfer of USD funds to Iran and that this was a "*common practice*" at Barclays.

757. As noted above, consistent with Barclays' "standard" procedures, when an Iranian payment was flagged by the Poole OFAC filter, Barclays' employees generally returned the flagged payment order message to the original remitting bank.

758. Barclays' employees used a specific fax cover sheet to advise the remitting area of Barclays that the payment message had been cancelled and would further identify the specific words in the payment message that had caused the message to be stopped by the Poole sanctions screening filter.

759. The Barclays fax cover sheet contained the following language:

> OFAC ITEM: Wording below is contained in the message and does not comply with the Office of Foreign Assets Control regulations applicable to all payments sent via the U.S.A. Payments to U.S.A. must NOT contain the word listed below.

760. Subsequently, because Barclays was advising the remitting bank of the prohibited language, some of these payment order messages would thereafter be re-sent by the remitting bank on the SWIFT-NET network without the "offending" language.

761. This deliberate omission enabled the payment order message to pass through the Poole sanctions screening filter without being blocked, and then clear and settle in USD funds by Barclays' New York branch and unwitting U.S. financial institutions.

762. In November 2001, the use of the fax cover sheet was identified by Barclays' internal auditors as problematic because (according to a Barclays internal audit report) "without adequate guidance the recipient of the fax advice may not be aware of the implications and may merely remove the offending text and re-submit the payment without any wider consideration."

763. In early 2002, as a result of this internal audit report, the language of the fax template was re-worded in an attempt to mitigate these issues. The fax language was changed to:

> OFAC ITEM: Wording below is contained in the message and does not comply with the U.S.A. / U.K. / E.C. / U.N. Sanctions.

764. Despite the altered wording in the fax cover sheet, no implementing guidance was circulated, and Barclays' "standard" practices nevertheless continued, as did the resubmission of prohibited OFAC-sanctioned transactions with the offending text removed.

765. Barclays' employees generated internal correspondence that documented Barclays' awareness and acceptance of the fact that transactions were being processed via MT 202 cover payments for the specific purpose of hiding the identity of Iranian entities in order to ensure that Barclays could continue its unfettered processing of USD funds transfers involving Iranian entities through Barclays' New York branch.

766. For example, one Barclays employee explained in an email:

> [W]e can get around [OFAC seizure] by sending only cover payments to US banks and then make MT103 direct to beneficiary's bank. The MT202 cover must not mention of [sic] the offending entity which could cause funds to be seized. A good example is Cuba which the US says we shouldn't do business with but we do.

767. Barclays' employees understood the advantage of using bank-to-bank cover payments. The cover payment message format (MT 202), with its limited information fields, was a better mechanism to process OFAC-prohibited transactions than using a more detailed serial payment message format (MT 103).

768. A Barclays employee noted in an email: "If we were to route the payment via the serial payment method ... the payment would clearly be seized by the US authorities" but by using cover payments, "the US Treasury [would] remain blissfully unaware of [the payment's] existence."

769. In December 2002, internal correspondence also brazenly acknowledged Barclays' use of MT 202 cover payment messages to detour U.S. Iranian sanctions, stating:

> To circumvent US legislation, [Barclays is] currently rout[ing] US$ items for sanctioned institutions via unnamed account numbers, without mention of the sanctioned party. For customer transfers, payment cover is routed via MT202 to New York, naming only the account holding bank. A direct MT103 is them [sic] sent to the account holding bank. Further investigation suggests that we are carrying out this practice on behalf of four [Iranian bank] customers….

770. A January 2004 report provided to Barclays' Group Risk Oversight Committee noted that a recent failure "illustrat[ed] why the whole sanctions process needs to be reviewed and brought up to date."

771. In July 2004, an internal assessment of Barclays' payments processing explained:

> Cover payments are an issue for this project as they are effectively a way of by passing [sic] sanctions.... There is nothing in these payment messages [MT 103 and MT 202] that identifies them as linked for the purpose of screening.

772. In April 2005, Barclays noted in an internal memo the risk of using MT 202 cover payments rather than MT 103 serial payments, and also acknowledged that other financial institutions such as the Western Bank Defendants facilitated payments for Iran in the same manner:

> Changing to different message types would be much more expensive to us. *Moral risk exists if we carry on using cover payments but that is what the industry does.* I[n] M[y] H[umble] O[pinion] we should carry on using cover payments and accept that there is a risk of these being used on occasion to hide true beneficiaries (who may or may not be sanctioned individuals or entities). [Emphasis added.]

773. In the spring of 2006, Barclays' senior management learned that four cover payments involving sanctioned parties had been routed through Barclays' New York branch and were processed because the cover payments did not mention the sanctioned beneficiary or originator.

774. Throughout this entire time period, Barclays knew that Iran was a designated State Sponsor of Terrorism and knew that Barclays was facilitating unlawful payments on behalf of Iran in furtherance of the Conspiracy.

775. Barclays also continued to facilitate unlawful payments on behalf of Bank Saderat *after* Barclays knew that Bank Saderat had been designated an SDGT for enabling the transfer of USD funds to Hezbollah.

776. Barclays also continued facilitating unlawful Eurodollar payments on behalf of Bank Melli *after* Barclays knew that Bank Melli had been designated by the United States in part for its enabling the transfer of USD funds to the IRGC.

777. On August 18, 2010, DOJ announced that Barclays had entered into a Deferred Prosecution Agreement with federal and New York State prosecutors and agreed to forfeit $298 million dollars in connection with violations of IEEPA and TWEA.

778. A criminal information was filed on August 16, 2010, in the U.S. District Court for the District of Columbia charging Barclays with one count of violating the IEEPA, and one count of violating TWEA. Barclays waived indictment, agreed to the filing of the information, and accepted and acknowledged responsibility for its criminal conduct.

779. In the press release announcing the DPA, then-FBI Assistant Director-in-Charge Janice K. Fedarcyk was quoted stating:

> Barclays Bank has admitted a decade-long pattern of violating U.S. banking laws, and taking certain steps to conceal prohibited transactions. Corporate responsibility entails more than just acting discreetly on behalf of one's clients. It means, first and foremost, acting lawfully.

K. DEFENDANT STANDARD CHARTERED BANK'S AGREEMENT TO AND PARTICIPATION IN THE CONSPIRACY

1. Standard Chartered Bank ("SCB") Conspired to Conceal Iran's Financial Activities and Transactions from Detection, Scrutiny, and Monitoring by U.S. Regulators, Law Enforcement, and/or Depository Institutions.

780. Defendant SCB provided, *inter alia*, trade-finance, Eurodollar and foreign exchange banking services to Iranian clients starting in or about 1993.

781. At some point thereafter, SCB began formulating plans to participate in and further the Conspiracy with Iran.

782. For example, on June 1, 1995, SCB's General Counsel wrote an e-mail advising SCB's regulatory compliance staff: "if SCB London were to ignore OFACs regulations AND SCB NY were not involved in any way & (2) had no knowledge of SCB Londons [sic] activities & (3) could not be said to be in a position to control SCB London, then IF OFAC discovered SCB London's [sic] breach, there is nothing they could do against SCB London, or more importantly against SCBNY."

783. The SCB General Counsel also instructed that a memorandum containing this plan was "highly confidential & MUST NOT be sent to the US."

784. In the ensuing years, Standard Chartered Bank actively conspired with the CBI, Bank Melli Iran, Bank Saderat plc's predecessor (Iran Overseas Investment Bank) and many other entities to assist Iran evade U.S. sanctions.

785. Standard Chartered Bank's role in the Conspiracy grew dramatically in early 2001, when the CBI approached SCB to act as the Central Bank of Iran's recipient bank for U.S. dollar proceeds from daily oil sales made by the NIOC in the Eurodollar market.[40]

[40] At some point, SCB Dubai also opened a Eurodollar credit facility for the CBI.

786. An e-mail dated February 19, 2001, from SCB's Head of Inbound Sales, Institutional Banking, characterized the CBI's solicitation of Standard Chartered as "*very prestigious*" because "*in essence, SCB would be acting as Treasurer to the CBI ...*"

787. Thus, Standard Chartered Bank was knowingly laundering billions of dollars in violation of multiple U.S. laws for the benefit of, among others, the IRGC.

788. In a follow up e-mail dated March 23, 2001, SCB's Group Legal Advisor wrote to its Product Manager, Corporate & Institutional Banking and its General Counsel (the e-mail was also forwarded to SCB's Group Head of Audit) that "our payment instructions [for Iranian Clients] should not identify the client or the purpose of the payment."

789. Standard Chartered Bank and the CBI quickly developed operating procedures for USD funds transfers to mask the involvement of Iranian entities in payment orders sent to Standard Chartered's New York branch ("SCB-NY").

790. When the beneficiary bank of a CBI Eurodollar payment transaction was an Iranian bank, SCB-London would send a SWIFT-NET MT 100 or MT 103 to the beneficiary bank's non-U.S., non-Iranian correspondent bank with full details of the Iranian beneficiary bank, and a *separate* MT 202 to SCB-NY with no mention of the Iranian beneficiary bank.

791. In fact, SCB-London set up routing rules within its payment system to route all incoming SWIFT-NET messages from the CBI to a repair queue, meaning that the payments were subject to manual review and processing by wire operators, to prevent Standard Chartered Bank - London from automatically processing outbound payment instructions for clearance and settlement in the United States with a reference to the CBI in the payment message.

792. Standard Chartered Bank - London's payment processing team initially instructed the CBI to insert Standard Chartered Bank - London's SWIFT-NET BIC address (identified as

SCBLGB2L) in field 52 (ordering institution) of its incoming payment order messages so that SCB's payment system would not populate that field with the CBI's SWIFT-NET BIC address (identified as BMJIIRTH).

793. When the CBI failed to remove its BIC address and insert Standard Chartered's BIC address into each SWIFT-NET message, Standard Chartered Bank - London wire operators would manually change field 52 to reference SCB - London's BIC in order to mask the CBI's involvement in the payments.

794. Standard Chartered Bank's willingness to further the Conspiracy in this manner attracted more illicit business.

795. As early as February 2002, several additional Iranian banks approached Standard Chartered Bank - London to discuss the possibility of opening new accounts.

796. SCB - London's Legal, Compliance, and Cash Management groups identified the need for written procedures for the operation of these additional Iranian banks' dollar-denominated accounts.

797. SCB's central role in the Conspiracy was memorialized in an internal memorandum regarding SCB's procedures for processing payments sent through the United States from the Iranian banks.

798. The document was entitled "Standard Chartered Bank Cash Management Services UK - Quality Operating Procedure: Iranian Bank Processing."

799. It was first issued to SCB London staff on February 20, 2004, and included detailed instructions regarding the omission of the Iranian remitting bank's BIC:

> Ensure that if the field 52 of the payment is blank or that of the remitting bank that it is overtyped at the repair stage to a "." (Note: if this is not done then the Iranian Bank SWIFT code may appear - depending on routing - in the payment message being sent to [SCB-NY]).

800. In addition to inserting a "." in field 52, the memorandum also instructed staff to use cover payments to process Iranian bank payments, which resulted in SCB London omitting any reference to the involvement of Iranian beneficiaries or beneficiary banks in SWIFT-NET payment order messages sent to Standard Chartered Bank's New York branch.

801. This element of the Conspiracy was particularly important to Defendant Bank Saderat Plc which repeatedly served as the Reimbursing Bank on Letters of Credit for other Iranian banks that were financing various illegal, sanctions-evading transactions on behalf of the IRGC and MODAFL through the United States.

802. Approximately 60,000 payments related to Iran, totaling **$250 billion**, were eventually processed by Standard Chartered Bank as part of the Conspiracy.

803. An e-mail dated March 9, 2003, from SCB's Head of Transactional Banking Solutions, UK/Europe Corporate & Institutional Banking to several of SCB's wholesale bank business managers indicates that Standard Chartered Bank learned that another bank was "*withdrawing their services*" with one of its Iranian client banks "primarily for reputational risk reasons."

804. In a memorandum accompanying the news of the aforementioned bank's reduction in Iranian business entitled "Summary of the Risks/Issues to be Addressed with Regard to Iranian Bank USD Clearing that Require Management Direction from Middle East Senior Management Team," the risks posed by additional Iranian business that might "trigger an action" from OFAC, "leaving SCB exposed, with potential reputational damage" were considered, but ultimately rejected in favor of pursuing additional Iranian business.

805. An October 15, 2003 e-mail from SCB's Manager, Cash Management Services, London to SCB's Product Manager, Corporate & Institutional Banking and its Head of Cash

Management Services, UK (forwarded to SCB's Head of Legal & Compliance, Americas and Head of Legal for Corporate & Institutional Banking) outlined how the CBI was instructed to "send in their MT 202's with a [SCB London's business identifier code] as this is what we required them to do in the initial set up of the account. Therefore, the payments going to NY do not appear to NY to have come from an Iranian Bank."

806. When Standard Chartered Bank anticipated that its business with the Iranian Bank Co-conspirators, including Defendant Bank Saderat Plc, would grow too large for SCB employees to manually "repair" the payment order messages for New York bound wire transfers, SCB automated the process by building an electronic repair system with "specific repair queues" for each Iranian client.

807. Standard Chartered Bank's payment "Quality Operations Procedures" manual contained instructions on how to manually "repair" or "over-type field 52 as [SCB London]" in SWIFT-NET MT 202 payment message fields to hide CBI's role as originator of the MT 202 cover payment transactions SCB was processing through New York in USD funds.

808. In October 2004, SCB consented to a formal enforcement action and executed a written agreement with the N.Y. State Banking Department and the Federal Reserve Board of New York ("FRB-NY"), which required SCB to adopt sound Bank Secrecy Act and Anti-Money Laundering ("BSA/AML") practices with respect to foreign bank correspondent accounts (the "Written Agreement").

809. The Written Agreement arose as a result of identified flaws in AML risk controls at Standard Chartered Bank's New York branch and it required SCB to adopt sound AML practices with respect to foreign bank correspondent accounts.

810. The Written Agreement also required SCB to hire an independent consultant to

conduct a retrospective transaction review for the period of July 2002 through October 2004.

811. The review was intended to identify suspicious activity involving accounts or transactions at, by, or through Standard Chartered Bank's New York branch.

812. Standard Chartered Bank failed to inform the N.Y. State Banking Department and the Federal Reserve Board of New York that its London and Dubai operations were secretly clearing hundreds of billions of dollars through Standard Chartered Bank's New York branch at the same time that it was promising to reform its AML practices.

813. SCB also failed to inform the N.Y. State Banking Department and the Federal Reserve Board of New York that its London, Dubai, Bahrain, Singapore and Hong Kong operations were secretly helping MODAFL and the IRGC evade U.S. sanctions at a time when they were illegally acquiring a wide range of U.S. equipment and technologies, including components for IEDs and EFPs used to kill and maim Coalition Forces in Iraq.

814. Standard Chartered Bank retained Deloitte & Touche LLP ("Deloitte") to conduct the required "independent" review and to report its findings to the regulators.

815. On August 30, 2005, and again on September 17, 2005, Deloitte provided Standard Chartered Bank confidential historical transaction review reports that Deloitte had prepared for two other major foreign banking clients that were under investigation for OFAC violations and money laundering activities.

816. Deloitte's reports contained detailed and highly confidential information concerning foreign banks involved in illegal U.S. dollar clearing activities.

817. SCB then asked Deloitte to delete from its draft "independent" report any reference to certain types of payments that could ultimately reveal Standard Chartered Bank's illegal Iranian-related practices.

818. In an e-mail dated October 1, 2005, SCB's Group Head of Legal & Compliance, Wholesale Bank, forwarding the *Quality Operating Procedure* to SCB's Group Head of Compliance and Regulatory Risk, its Group Legal Advisor and its Head of Financial Crime Risk Systems and Monitoring, observed that "read in isolation, is clearly ... designed to hide, deliberately, the Iranian connection of payments."

819. A few days later, in an e-mail dated October 8, 2005, Deloitte's Global Leader of Anti-Money Laundering/Trade Sanctions Division wrote to SCB's Head of Compliance, that Deloitte had "agreed" to accede to Standard Chartered Bank's request that Deloitte delete from its draft "independent" report any reference to certain types of payments that could ultimately reveal Standard Chartered Bank's illegal Iranian U-Turn practices because "this is too much and too politically sensitive for both SCB and Deloitte. That is why I drafted the watered-down version."

820. In a December 1, 2005 internal memorandum entitled "*Project Gazelle*," SCB's Group Head of Compliance and Regulatory Risk and its CEO in the United Arab Emirates wrote to SCB's Group Executive Director for Risk and its Group Head of Global Markets, acknowledging that Standard Chartered Bank repair procedures for U-Turn exemption transactions did "not provide assurance that it does not relate to a prohibited transaction, and therefore SCB NY is exposed to the risk of a breach of sanctions."

821. A February 23, 2006 internal memorandum entitled "Iranian Business" sent from Standard Chartered Bank's General Counsel to SCB's Audit and Risk Committee confirmed SCB's continued recognition that the Conspiracy was expressly designed to enable Iran and the Iranian Bank Co-conspirators (including Defendant Bank Saderat Plc) to evade U.S. detection of their transactions and confirmed that "certain US$ clearing transactions handled in London were processed with the name of the Iranian Bank excluded or removed from the 'remitter field'" despite

the "requirement that due diligence in respect of 'U-turn' payments should be undertaken by our office in New York."

822. In September 2006, New York State regulators requested that SCB provide them with statistics on Iranian U-Turns SCB handled, including the number and dollar volume of such transactions for a 12-month period.

823. In response, SCB searched its records for 2005 and 2006.

824. In a September 26, 2006 email from SCB's Project Manager for the Lookback Review to SCB's Head of Cash Management Services (2002-2005) and Head of Compliance (2005-2007) at Standard Chartered Bank's New York branch, SCB's Head of Operations and Head of Cash SCB identified 2,626 transactions totaling over $16 billion (for Iranian banks).

825. Faced with the prospect of disclosing *billions* of dollars in Iranian transactions, Standard Chartered Bank's New York branch's Head of Compliance was directed by his superiors at SCB to provide instead only ***four days*** of U-Turn data to regulators; these four days were masquerading as a log covering two-years of transaction data.

826. In October 2006, the CEO for SCB's U.S. Operations e-mailed the SCB Group Executive Director in London:

> Firstly, we believe [the Iranian business] needs urgent reviewing at the Group level to evaluate if its returns and strategic benefits are . . . still commensurate with the potential to cause very serious or even catastrophic reputational damage to the Group. Secondly, there is equally importantly potential of risk of subjecting management in US and London (e.g. you and I) and elsewhere to personal reputational damages and/or serious criminal liability.

827. SCB's Group Executive Director responded (as quoted by a Standard Chartered Bank's New York branch officer): "You f---ing Americans. Who are you to tell us, the rest of the world, that we're not going to deal with Iranians."

828. In 2007, SCB successfully convinced the N.Y. State Banking Department and

FRBNY to lift their consent order on SCB based on the watered-down D&T report and its other fraudulent disclosures.

829. As noted above, from approximately January 2001 through 2007, SCB transferred at least *$250 billion* through Standard Chartered Bank's New York branch on behalf of the Iranian Bank Co-conspirators, including Bank Melli Iran and the CBI, as well as Defendant Bank Saderat Plc.

830. Standard Chartered Bank's New York branch processed approximately **60,000 wire transfers** on behalf of the Iranian Bank Co-conspirators, with roughly half of the transactions originating with SCB's London office, and the other half with SCB's branch in Dubai, UAE.

831. In early 2009, after being contacted by U.S. law enforcement authorities, SCB conducted yet another "internal investigation" into its OFAC sanctions screening procedures, business practices and technology.

832. Nonetheless, Standard Chartered Bank's New York branch was the conduit for at least 50 post-U.S. designation transactions on behalf of IRISL and its various front companies through June 2010.

833. As of 2011, however, even after its internal investigation and open law enforcement investigations commenced in the U.S., the New York State Banking Department still found that Standard Chartered Bank's New York branch had:

a. No documented evidence of investigation before the release of funds for transactions with parties whose names matched the OFAC-sanctioned list; and

b. Outsourced Standard Chartered Bank's New York branch's entire OFAC compliance process to Chennai, India, with no evidence of any oversight or communication between the Chennai and Standard Chartered Bank's New York branch.

2. SCB Facilitated Transactions on Behalf of MODAFL, Mahan Air and Other Instrumentalities of Iranian State-Sponsored Terror (Including a Hezbollah Affiliated Entity) in Furtherance of Numerous Violations of the U.S. Trade Embargo, Thereby Substantially Contributing to the Plaintiffs' Injuries.

834. From at least 2001 to 2007, SCB illegally facilitated more than 1,300 Letters of Credit through stripping or cover payment methods that purposefully concealed the participation of Iranian counterparties in the transactions.[41]

835. Many of those LCs were issued for the benefit of Iran's military / terror apparatus, facilitating and financing the IRGC's, MODAFL's and Hezbollah's illegal acquisitions of materials and technologies, including materials unlawfully obtained from the United States and components for IEDs and EFPs used against Coalition Forces in Iraq.

836. SCB knowingly facilitated and financed the illegal export to Iran of U.S.-manufactured, export-controlled defense and dual-use products worth tens of millions of dollars. These were acquired by various Iranian-controlled front companies on behalf of, *inter alia*, the following entities:

a. Mahan Air;

b. Four MODAFL subsidiaries: the AIO, the IACI, the IHRSC, and HESA;

c. The Iran Power Development Company ("IPDC"), MAPNA and Zener Electronics Services (an agent of Hezbollah);

d. NIOC and several of its subsidiaries; and

e. Khoram Sanat Producing Co. – Iran.

837. None of these aforementioned entities is (or was) a legitimate agency, operation, or program of the Iranian government.

[41] A more accurate accounting would probably exceed 9,000 trade-finance and Eurodollar payment transactions.

838. On the contrary, Mahan Air is an SDGT that, according to the U.S. government, (1) "facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq;" (2) "facilitated IRGC-QF arms shipments"; and (3) "transported personnel, weapons and goods on behalf of Hezbollah. [sic]"

839. Mahan Air was also later identified as the conduit to Iran of *thousands* of radio frequency modules recovered by Coalition Forces in Iraq from IED devices that were used to target, kill and maim U.S. and Coalition Forces.

840. Similarly, MODAFL is the principal procurement arm of Iran's military and terror apparatus.

841. The Mapna group is also a key component of MODAFL and the IRGC's procurement chain.

842. Abbas Aliaabadi, Chairman of Mapna International FZE and President of the Mapna Group, is a former member of the Iranian Ministry of Construction Jihad and of the Iranian Air Force. Aliaabadi was also a key member of the Ministry of Culture & Islamic Guidance instrumental in the creation of Hezbollah and has close links to the IRGC.

843. During the relevant time period, the National Iranian Oil Company was not only controlled by , and an agent of, the IRGC but also served as the lifeblood of the Iranian regime's illicit financing activities, providing it with access to billions of dollars in oil and natural gas revenues that enabled the IRGC to gain access (through the Conspiracy) to the global financial system.

844. Standard Chartered Bank knowingly conspired with Iran to facilitate illicit trade for all of these entities in violation of U.S. law, thereby substantially assisting Iran in its criminal (and specifically terrorist) conduct in Iraq. The foreseeable consequence of that assistance was to enable

Iran, the IRGC and Hezbollah to kill or wound, or try to kill, or conspire to kill more Americans in Iraq.

845. At all relevant times, SCB was fully aware of both the Iran Trade Regulations and the Export Administration Regulations, the U.S. State Department's United States Munitions List ("USML") and their many restrictions.

a. Standard Chartered Knowingly Provided Illegal Financing to Mahan Air.

846. Between 2000 and 2006, Standard Chartered Bank facilitated LCs for the benefit of Mahan Air totaling more than $120 million.

847. As noted above, the Treasury Department designated Mahan Air in 2011, finding that:

> Mahan Air also facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel.
>
> Mahan Air crews have facilitated IRGC-QF arms shipments. Funds were also transferred via Mahan Air for the procurement of controlled goods by the IRGC-QF.
>
> In addition to the reasons for which Mahan Air is being designated today, Mahan Air also provides transportation services to Hezbollah [sic], a Lebanon-based designated Foreign Terrorist Organization. Mahan Air has transported personnel, weapons and goods on behalf of Hezbollah [sic] and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hezbollah [sic].

848. Mahan Air also transported to Iran *thousands* of radio frequency modules illegally imported by OPTO Electronics in Singapore, NEL Electronics PTE Ltd. and Corezing International PTE Ltd. from the United States.[42]

[42] *See*, Superseding Indictment in *U.S. v. Larijani* at: https://www.justice.gov/opa/file/837996/download.

849. These modules were recovered by Coalition Forces in Iraq from IED devices that were used to target U.S. and Coalition Forces.

850. The modules had encryption capabilities and a particularly long range that allowed Special Groups operatives to operate them across significant distances.

851. In 2008, Mahan Air transported the IED components from Singapore and Thailand to Tehran, Iran.

852. Under Secretary of Commerce Eric L. Hirschhorn described this supply chain as "egregious conduct by… foreign companies and individuals who have endangered the lives of U.S. and coalition forces in Iraq."

853. Five LCs facilitated by Standard Chartered Bank listed Mahan Air as the "Applicant" and involved the illegal acquisition of materials ranging from aviation parts to a U.S. shipment of an Airbus A320.

854. The Issuing Banks for the LC included Defendant Bank Saderat Plc, Bank Melli Iran and Bank Sepah.

855. SCB's New York branch served as the clearing bank for these LCs.

856. Furthermore, in another transaction, Mahan Air was the listed Beneficiary of a $21 million dollar LC facilitating the leasing of several second-hand Airbus A320s from Europe.[43]

857. In facilitating these trade-finance transactions, often for explicitly "Non-EAR 99" goods of U.S. origin – i.e. products on the Commerce Control List, Standard Chartered Bank knew that it was (1) working with Iranian banks, (2) concealing the Iranian connection to the trade-

[43] Mahan Air was the target of a Temporary Denial Order ("TDO") by the U.S. Department of Commerce in March 2008 for, *inter alia*, "knowingly re-exporting to Iran three US-origin aircraft, specifically Boeing 747." The Bureau of Industry and Security's TDO was renewed subsequently several times.

finance and Eurodollar transactions and (3) facilitating the unlawful delivery of these U.S. export controlled parts or products to Iranian entities in Iran.

858. For at least two transactions facilitated on behalf of Mahan Air (including one for export controlled goods of entirely U.S. origin), Credit Suisse in Zurich facilitated the payment on the LC to Standard Chartered Bank, Dubai, and on at least one of those transactions, the payment was routed by Credit Suisse in Zurich through New York on behalf of Bank Melli in the UAE with the transaction being cleared and settled in USD funds by Standard Chartered Bank's New York branch.

859. On one occasion, Mahan Air purchased an Airbus (aircraft) using Blue Sky Aviation as its intermediary. Standard Chartered Bank, Dubai provided the nearly $30 million to Blue Sky for the purchase, and Bank Sepah (Iran) guaranteed the payment through a re-payment made by Credit Suisse on its behalf in 2006.

860. The front companies listed as beneficiaries of the LCs facilitated by Standard Chartered Bank included Sirjanco Trading LLC ("Sirjanco") and Blue Sky Aviation Co FZE ("BSA FZE" or "BSA"), both later designated by the U.S. Treasury as SDGTs, in part, because of the illegal sanctions evading conduct facilitated and enabled by Standard Chartered Bank.

861. Hamidreza Malekouti Pour served simultaneously as the Regional Manager for Mahan Air in the UAE and Managing Director of Sirjanco and BSA FZE – effectively demonstrating how these companies are all part of the same IRGC supply chain. Pour has also been designated as an SDGT for, *inter alia*, supplying equipment to the IRGC-QF.

862. When designated by the U.S. Treasury Department in 2013 as a Specially Designated Global Terrorist,[44] Sirjanco was described as "a United Arab Emirates-based company

[44] Sirjanco was previously the target of a Temporary Denial Order by the U.S. Department of Commerce in 2011.

designated pursuant to E.O. 13224 for acting for or on behalf of Mahan Air. Sirjanco was established specifically to serve as a financial front for Mahan Air. Sirjanco has also served as a front for Mahan Air's acquisition of aircraft. Additionally, Iran's IRGC-QF has used Sirjanco to procure sanctioned goods."

863. A 2005 LC facilitated by Standard Chartered Bank listed Mahan Air as the Applicant, and Sirjanco as the beneficiary, for a total of $32,500,000.

864. Bank Melli financed the payment through Credit Suisse, which sent the payment order through New York (clearing and settling in USD funds through Standard Chartered Bank's New York branch).

865. The payment was made by Standard Chartered Bank, Dubai to Sirjanco's account with Bank Saderat, Dubai.

866. At least two other LCs facilitated by Standard Chartered Bank listed Mahan Air as the Applicant, and Blue Sky Aviation as the Beneficiary, for a total of over $60,000,000.[45] All told, between 2000 and 2006, Standard Chartered Bank facilitated at least 11 LCs for the "Blue Sky Group" for a total of more than $125 million.

867. When the U.S. Treasury Department designated Blue Sky Aviation in 2014, it described it as "a UAE-based company that is owned or controlled by Mahan Air and acts for or on behalf of the airline. BSA FZE's primary function has been to serve as a payment channel for Mahan Air to obscure the origination of funds. Mahan Air has used BSA to make payments to oil suppliers, and purchase aircraft, engines, and parts."

868. In sum, Standard Chartered Bank was vital to Mahan Air's continued operations and its ability to facilitate travel by IRGC-QF officers and arms shipments in and out of Iraq,

[45] Plaintiffs' estimates are based on only one Promontory report. SCB's historical relationship with the Blue Sky Group was the subject of a separate Promontory Report not (yet) available.

transport IED technologies into Iraq as well as transit personnel, weapons and goods on behalf of Hezbollah, which helped facilitate terrorist attacks in Iraq during the relevant time period.

869. While neither Mahan Air nor Blue Sky Aviation was designated as a terrorist at the time the LCs identified above were financed, Standard Chartered Bank engaged in criminal conduct in furtherance of the Conspiracy in order to aid these IRGC supply chain entities to evade U.S. sanctions knowing that its own conduct was illegal.

870. At the time it agreed to engage in overt acts in furtherance of the Conspiracy, Standard Chartered Bank knew that: (1) Iran was a U.S.-designated State Sponsor of Terrorism; (2) the U.S. had imposed strict sanctions and export controls on Iran and Iranian trade; (3) Mahan Air was seeking to illegally acquire U.S. export controlled defense and dual-use materials; and (4) Mahan Air was using front companies to do so.

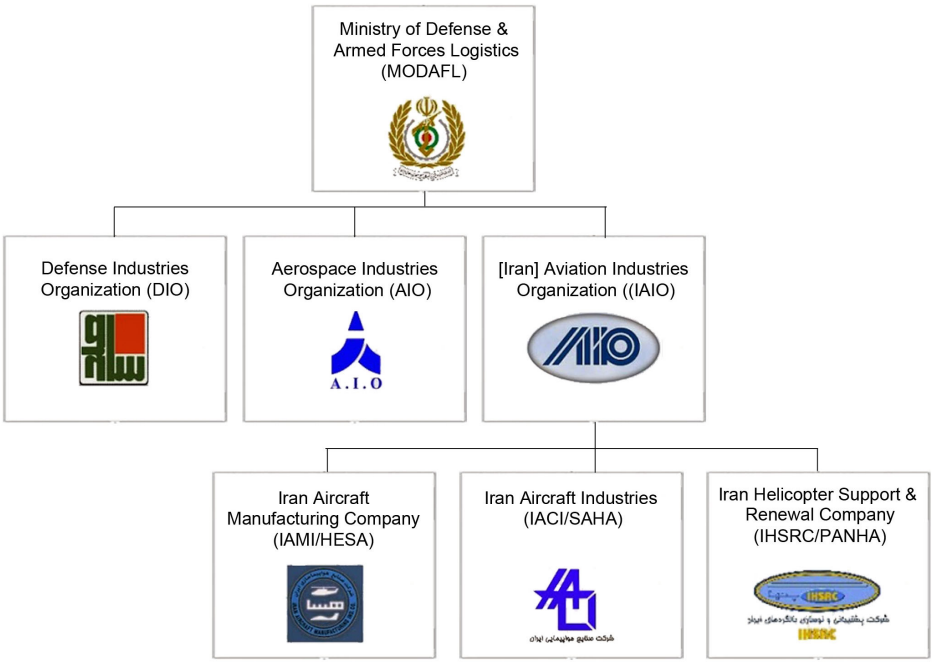
871. In sum, Standard Chartered Bank affirmatively chose to facilitate Iran's illegal conduct and provide material support to its terror apparatus, including Mahan Air, Blue Sky Aviation and Sirjanco. All of these entities were later designated as SDGTs in part because of the types of trade-finance and Eurodollar transactions facilitated by Standard Chartered Bank.

b. Standard Chartered Knowingly Provided Illegal Financing to MODAFL Companies: AIO, IACI, IHRSC and HESA.

872. Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) operates the [Iran] Aviation Industries Organization (IAIO), the Aerospace Industries Organization (AIO) and the Defense Industries Organization (DIO). MODAFL was designated by the United States on October 25, 2007.[46]

[46] MODAFL was also sanctioned, pursuant to the Arms Export Control Act and the Export Administration Act, in November 2000.

873. The AIO was designated on June 28, 2005 for weapons proliferation. Standard Chartered Bank knowingly provided financing for both the AIO directly, and for 3 major sub-agencies of MODAFL's IAIO: the Iran Aircraft Industries **("**IACI")[47] a/k/a SAHA, the Iran Helicopter Support and Renewal Company ("IHSRC") a/k/a PANHA, and the Iran Aircraft Manufacturing Industrial Company ("IAMI" a/k/a "HESA"). Support for any of these entities, as sub-agencies of MODAFL and the IAIO, was not for legitimate agencies, operations or programs of Iran.



i. SCB Trade-Finance Transactions with MODAFL's Aerospace Industries Organization (AIO)

874. In 2002, Standard Chartered Bank facilitated an LC for MODAFL's Aerospace Industries Organization that cleared through SCB's New York branch valued at $57,662 USD for

[47] IACI was also formerly listed by the European Union on July 26, 2010, and described as an entity that "[m]anufactures, repairs, and conducts overhauls of airplanes and aircraft engines and procures aviation-related parts often of US-origin typically via foreign intermediaries. IACI and its subsidiaries also have been detected using a worldwide network of brokers seeking to procure aviation-related goods." IACI was also formerly sanctioned by Switzerland, Norway, Japan, Australia, Canada, and the UK. It was designated by the United States in 2013.

the illegal purchase of U.S. export-controlled goods.[48]

875. That transaction was not for the benefit of any legitimate agencies, operations or programs of Iran.

ii. SCB Trade-Finance Transactions with MODAFL's [Iran] Aviation Industries Organization (IAIO)

876. On numerous additional occasions, Standard Chartered Bank illegally facilitated trade-finance and Eurodollar transactions on behalf of other MODAFL sub-agencies, including HESA.

877. On September 17, 2008, the U.S. Treasury Department designated HESA,[49] finding that it is:

> owned or controlled by MODAFL, and also because it has provided support to the Iranian Revolutionary Guard Corps (IRGC). The IRGC, which was designated under Executive Order 13382 on October 25, 2007, is considered to be the military vanguard of Iran and has been outspoken about its willingness to proliferate ballistic missiles capable of carrying WMD.
>
> HESA utilizes its own facilities for the inspection, maintenance, repair overhaul research, development, and manufacture of military and civilian aircraft and related military logistic systems. HESA conducts research on, development of, production of, and flight operations for unmanned aerial vehicles (UAVs) in Iran. The IRGC utilizes the "Ababil" UAV, manufactured by HESA. HESA produces different variants of the Ababil UAV, which can be used for surveillance and attack. Farasakht Industries is a subsidiary of HESA that specializes in the manufacturing of various aerospace tools and equipment.

[48] AIO was reportedly responsible for developing anti-tank guided weapons; artillery rocket systems; anti-tank missiles; precision machining and metal forming for a variety of Iranian weapons systems.

[49] HESA was previously identified in a document distributed by the German government in July 2005, warning of its potentially illicit activities. It was also identified by the UK government in February 1998 as having procured goods and/or technology for WMD programs.

(A) SCB's Trade-Finance Transactions with MODAFL-IAIO Front Company Downtown Trading Ltd.

878. Between 1998 and 2002, Standard Chartered Bank facilitated ten LCs involving a company based in Malaysia (and with links to a same named company registered in the U.K.), Downtown Trading Ltd ("Downtown Trading").

879. The total value of these ten LCs involving Downtown Trading amounted to $1,067,575.

880. MODAFL-IAIO's subsidiary Iran Aircraft Industries ("IACI") was the Applicant on these LCs, i.e. the purchaser of the U.S. origin aircraft engine parts in question for seven of these transactions, while Downtown Trading was the reported Beneficiary.

881. In most or all of these transactions, primarily those for 2002, Bank Sepah (Iran) served as the Issuing Bank, Bank Sepah (London) served as the Reimbursing Bank, SCB Dubai served as the Negotiating Bank, and SCB's New York branch helped facilitate the transactions by serving as the Clearing Bank.

882. With respect to at least four of these transactions, the U.S. aircraft parts were transported by Iran Air, later designated as "a commercial airline used by the IRGC and Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) to transport military related equipment…. Iran Air has provided support and services to MODAFL and the IRGC through the transport and/or transfer of goods for, or on behalf of, these entities."

883. IACI's illegal procurements were often financed by Bank Sepah (as the Issuing Bank), but Standard Chartered Bank in Dubai frequently served as the Negotiating Bank and SCB's New York branch usually served as the Clearing Bank for these same trade-finance transactions, in at least one case paying Citibank in New York the fund due.

884. Citibank then paid Maybank, Malaysia, which effected the ultimate payment to the Eurodollar account of Downtown Trading.

885. Standard Chartered Bank also facilitated similar LCs in USD funds for Downtown Trading after April 2005.

886. In facilitating these transactions – 70% of which explicitly involved export-controlled "Non-EAR 99" goods of U.S. origin (i.e. products on the Commerce Control List) – Standard Chartered Bank knew that it was: (1) working with Iranian banks; (2) concealing the Iranian connection to the transactions; (3) facilitating the unlawful delivery of goods on the U.S. Commerce Control List to Iran's military and/or the IRGC; and (4) that these transactions were not for legitimate agencies, operations, or programs of Iran.

(B) SCB's Trade-Finance Transactions with MODAFL-IAIO Front Company Mac Aviation

887. Mac Aviation is an Irish trading company incorporated in 1993 that purported to engage in the purchase and sale of aircraft and helicopter parts.

888. The company and its owners[50] were indicted in 2008 for, among other things, violations of the IEEPA, the ITR, and U.S. export controls.

889. During the relevant time period, Mac Aviation was a customer of Standard Chartered Bank in London.

890. According to the indictment, between June 2005 and July 2008 Mac Aviation solicited purchase orders from customers in Iran for U.S. origin aircraft parts and then forwarded these requests for the parts to U.S. companies.

[50] In 1994, one of the owners of Mac Aviation, Thomas McGuinn, was convicted by a Florida court for exporting defense products to Iran. He pled guilty and was sentenced on April 19, 1996, to time served and 3 years of supervision on release. McGuinn was also barred from receiving licenses for exporting U.S. defense articles.

891. The indictment further alleges that Mac Aviation wired funds to banks in the U.S. as payment for these parts and concealed from U.S. sellers the ultimate end-use and Iranian end-users of the purchased parts.

892. The indictment also alleges that Mac Aviation caused the export of these parts from the U.S. to third countries, including Malaysia, before sending their shipments onward to Iran.

893. At least one of those shipments, directed by Mac Aviation in February 2006, resulted in a shipment being made from a firm called Microset Systems Sdn Bhd in Kuala Lumpur, Malaysia, to Sasadja Moavanate Bazargani in Tehran, Iran, an alter ego of Iran's Defense Industries Organization (DIO), which had been designated by Germany, the United Nations, and the United States as a procurer of unlawful weapons components beginning as early as 2005.

894. As noted above, weapons caches seized from Special Groups by Coalition Forces in Iraq included many 107 mm artillery rockets with closely clustered DIO lot numbers and production dates between 2005 and 2007, as well as rounds and fuses for 60 mm and 81 mm mortars with DIO lot markings and 2006 production dates.

895. In another example, in January 2006, police in the southern Iraqi city of Amara, near the Iranian border, captured seventy blocks of TNT explosives and seventy-nine blocks of plastic explosive, which were used by the Special Groups as components of IEDs, all with markings and lot numbers showing that they were produced by DIO.

896. In July 2010, the DOJ obtained a 27-count superseding indictment in *USA v. Mac Aviation et al.* charging the company and its officers with:

> purchasing F-5 fighter aircraft parts, helicopter engines and other aircraft components from U.S. firms and illegally exporting them to Iran.…
>
> […] Beginning as early as August 2005… through July 2008, the defendants solicited purchase orders from customers in Iran for U.S.-origin aircraft engines and parts and then sent requests for aircraft components to

> U.S. companies. These parts included helicopter engines, aircraft bolts and vanes, and canopy panels for the F-5 fighter aircraft. The defendants wired money to banks in the U.S. as payment for these parts and concealed from U.S. sellers the ultimate end-use and end-users of the purchased parts.
>
> The defendants caused these parts to be exported from the U.S. to third countries like Malaysia before causing them to be transshipped to Iran. […]
>
> From 2005 [… to] 2006, the defendants caused canopy panels designed for the F-5 fighter aircraft, valued at approximately $44,500, to be exported from the U.S. to Iran. The defendants falsely stated that the end user for the F-5 panels was the Republic of Nigeria. Instead, the panels were sold by the defendants to Sasadja Moavanate Bazargani, in Tehran, Iran for $86,400. The purchase was arranged through the Iran Aircraft Manufacturing Industrial Company, known by its Iranian acronym as HESA.

897. According to the superseding indictment, Mac Aviation also shipped fifteen helicopter engines to Iran Aircraft Industrial Manufacturing Company ("HESA").

898. These included ten Rolls-Royce Model 250 C-20B turboshaft engines, and five Rolls-Royce Model 250 C-20R2 turboshaft engines.

899. Rolls-Royce Model 250 engines are used on HESA's 278 Shahed (military) helicopters (converted or adapted from the design of the American Bell 206B-III "Jet Ranger" and Bell 206L "Long Ranger" aircraft) flown by and developed for the IRGC.

900. Between 2001 and 2005, Standard Chartered Bank facilitated at least 21 LCs involving Mac Aviation for a total of close to $8 million.

901. In each case, Mac Aviation was the nominal purchaser of the aircraft parts (Applicant), and the listed importer was either Iran Aircraft Industries ("IACI"), Iran Helicopter Support and Renewal Industries ("IHSRC"), or Iran Aircraft Manufacturing Industrial Company ("HESA").[51]

[51] Iran used an Iranian national named Hossein Ali Khoshnevisrad as an intermediary. Khoshnevisrad used two Iranian companies – Ariasa AG (Tehran) and Onakish Co. (Kish Island, Iran) – to deal directly with Mac Aviation. Khoshnevisrad was arrested in the U.S. in 2009 and "charged with purchasing helicopter engines and advanced aerial

902. Most, if not all of these LCs appear to have been financed, at least in part, by: Bank Saderat in London (IOVB) serving as the Reimbursing Bank; Bank Refah Iran serving as the Issuing Bank; Standard Chartered Bank in London serving as the Advising Bank; SCB in Dubai serving as the Negotiating Bank; and Standard Chartered Bank's New York branch serving as the Clearing Bank.

903. Some of the transactions were financed through the CBI's Eurodollar credit line with Standard Chartered Bank.

904. The other transactions were financed through reimbursements in USD funds claimed by Standard Chartered Bank - London primarily from Defendant Bank Saderat Plc with funds deposited received into Standard Chartered Bank London's U.S. dollar account with Standard Chartered's New York branch for further credit to the Eurodollar account of Mac Aviation (SCB's customer).

905. Iran Air was often used to deliver the illegally procured equipment to Iran.

906. Notably, Bank Refah Iran was designated on February 17, 2011, by the U.S. Treasury Department for:

> providing financial services to the Iranian Ministry of Defense and Armed Forces Logistics (MODAFL) and the Iran Aircraft Manufacturing Industrial Company (HESA). In recent years, Bank Refah has facilitated millions of dollars of weapons-related purchases by MODAFL. These purchases included missiles and tanks and enabled Iran's leadership to maintain its fighter jets and submarines. Bank Refah also facilitated payments from HESA to businesses and individuals linked to Iran's weapons-related procurement.[52]

---

cameras for fighter bombers from U.S. firms and illegally exporting them to Iran using companies in Malaysia, Ireland and the Netherlands. Among the alleged recipients of these U.S. goods was ... HESA."

[52] Standard Chartered Bank maintained correspondent accounts for Bank Refah in Bangladesh, China, Hong Kong, India, Indonesia, Japan, South Korea, Malaysia, Qatar, Singapore, Sri Lanka, Taiwan, Thailand and UAE.

907. Standard Chartered Bank's financing of MODAFL's clandestine and illegal acquisition of U.S. military (aircraft) spare parts did not fund or facilitate Iran's legitimate agencies, operations, or programs.

908. Rather, Standard Chartered Bank actively participated in a criminal conspiracy to help Iran's military and terror apparatus obtain critical machinery and equipment and aircraft spare parts it desperately needed to sustain its violent and unlawful activities.

(C) SCB's Trade-Finance Transactions with MODAFL-IAIO Front Company Monarch Aviation (Singapore)

909. Monarch Aviation was an Iranian front company based in Singapore that was owned and controlled by husband and wife, Brian Douglas Woodford, a UK citizen, and Laura Wang-Woodford, a dual U.S. and UK citizen.

910. It purported to be a manufacturer, dealer, and repairer of aircrafts and related parts. At least during the period between 2001 and 2007, Standard Chartered Bank in Singapore ("SCB-Singapore) maintained accounts for Monarch Aviation, Brian Douglas Woodford, and Laura Wang-Woodford.

911. Monarch Aviation held at least one account at the SCB-Singapore Battery Road branch, under the account number ACU- 26-0-000106-3.

912. Defendant Credit Suisse's Singapore Branch at 80 Raffles Place also maintained a U.S. dollar account for Monarch Aviation with the account number K0100340.01.

913. On January 15, 2003, Woodford and Wang-Woodford were indicted for, among other things, violations of the IEEPA, and U.S. export control laws.[53]

[53] A Superseding Indictment was returned on May 22, 2008.

914. Laura Wang-Woodford was arrested on December 23, 2007, and later pled guilty to conspiring to violate the U.S. trade embargo by exporting U.S. origin aircraft components to Iran.

915. According to the Superseding Indictment, between January 1998 and December 2007, Monarch Aviation, Jungda International Pte Ltd. (a Singapore based successor to Monarch Aviation), Brian Douglas Woodford and his wife, Laura Wang-Woodford, exported U.S. aircraft parts to Singapore and Malaysia, and then re-exported those items to companies in Tehran, Iran, without obtaining the required U.S. government licenses, while falsely listing their companies as the ultimate recipients of the parts on export documents filed with the U.S. government.

916. Specifically, according to the Superseding Indictment and the U.S. Justice Department's Sentencing Recommendation, the funds transferred by Monarch Aviation paid for Boeing CH-47 ("Chinook") helicopter parts, including vane assemblies and bevel gears that were listed under category VIII on the United States Munitions List ("USML") and illegally exported to Iran.

917. The vane assemblies, part number 2-080-090-02 and national stock number ("NSN")[54] 2840-01-022-7142, and bevel gears, part number 2-080-013-03 and NSN 3020-00-860-7419, were manufactured by Honeywell International Inc., commercial and government entity ("CAGE")[55] code 99193, in Phoenix, Arizona.

---

[54] The U.S. National Stock Number (NSN) is a unique thirteen-digit numerical identifier assigned to each part used by the U.S. Department of Defense (DOD). The NSN system is managed by DOD's Defense Logistics Agency ("DLA"). The DLA system of NSNs was mandated by the 1952 Defense Cataloging and Standardization Act (Pub L No 82-436).

[55] The CAGE code is a unique identifier assigned to, *inter alia*, U.S. defense contractors and DOD maintenance facilities. The CAGE code provides a standardized method of identifying a given government or defense contractor facility at a specific location.

918. These export-controlled, U.S.-manufactured helicopter parts were used in Iran's fleet of Boeing CH-47 Chinook heavy-lift utility helicopters that were refurbished by HESA.

919. Iran's CH-47 helicopters are operated by the Islamic Republic of Iran Army Aviation ("IRIAA") and the Islamic Republic of Iran Air Force ("IRIAF").

920. The Superseding Indictment also listed the following parts, *inter alia*, that were illegally exported to Iran by Monarch Aviation: o-rings, shear bolts, bushings, and rotary wing shields.

921. The o-rings, identified by part numbers S6135-20059-102 (NSN 5331-01-270-1765) and S6135-20059-106 (NSN 5331-01-270-1766), were manufactured by Sikorsky Aircraft Corporation (CAGE code 78266) in Stamford, Connecticut.

922. These export-controlled, U.S.-manufactured parts were used in Iran's fleet of Sikorsky SH-3D ("Sea King") medium-lift utility/anti-submarine warfare helicopters that were refurbished by Iran HESA.

923. Iran's SH-3D helicopters are operated by the Islamic Republic of Iran Navy Aviation ("IRINA").

924. The following parts were manufactured by Bell Helicopter Textron, Inc. (CAGE code 97499) in Fort Worth, Texas:

a. Shear bolts, identified by part number NAS625-44 (NSN 5306-00-924-6261);

b. Bushings, identified by part number 205-030-477-11 (NSN 1560-00-413-1492); and

c. Rotary-wing shields, identified by part number 204-012-118-1 (NSN 1615-00-865-7914).

925. These export-controlled, U.S.-manufactured parts were used in the following Iranian rotary-wing aircraft:

a. Bell AH-1J ("Cobra") air-assault helicopters (refurbished by HESA);

b. Bell UH-1 ("Iroquois") utility transport helicopters (refurbished by HESA);

c. Iranian Helicopter Support and Renewal Company ("PAHNA") 2091 ("Toufan") air-assault helicopters (the PAHNA 2091 is an Iranian remanufactured version of the Bell AH-1J helicopter); and

d. PAHNA 2-75 ("Shabaviz") utility transport helicopters (the PAHNA 2-75 is an Iranian remanufactured version of the Bell UH-1 helicopter).

926. Iran's fleet of Bell AH-1J, Bell UH-1, PAHNA 2091 and PAHNA 2-75 helicopters are operated by the Iranian Revolutionary Guard Corps Air Force ("IRGC-AF") and IRIAA.

927. From 1998 to 2005 (and likely thereafter), Standard Chartered Bank facilitated at least 10 LCs financed by the CBI and Bank Refah with a total value of more than $1.5 million involving the shipment of U.S. origin aircraft parts sold by Monarch Aviation to MODAFL's sub-agencies Iran Aircraft Industries ("IACI"), Iran Helicopter Support and Renewal Co. ("IHSRC"), and HESA.

928. Defendant Bank Saderat Plc served as the Reimbursing Bank on most, if not all, of these transactions, which cleared through Standard Chartered Bank's New York branch on their way to Monarch Aviation's accounts at Standard Chartered in Singapore.

929. The aircraft parts were transported by Iran Air from Kuala Lumpur Airport, Malaysia, to Tehran Airport, Iran.

930. SCB in Dubai served as the Negotiating Bank, and funds from the financing were

paid to Monarch Aviation's account with Standard Chartered Bank, Singapore through SCB Singapore's account with Standard Chartered, London, which in turn received the funds into its U.S. Dollar nostro account with Standard Chartered Bank's New York branch from Standard Chartered Bank - Bahrain's Offshore Booking Unit ("OBU").[56]

931. In sum, various overseas branches of Standard Chartered Bank conspired with multiple MODAFL sub-agencies and Monarch Aviation, and used Standard Chartered Bank's New York branch to both assist Iran's military in illegally acquiring contraband U.S. goods and to illegally disguise the illicit financing of those acquisitions through Standard Chartered Bank's New York accounts.[57]

932. Standard Chartered Bank facilitated at least 316 additional transactions totaling $12,110,565 in USD funds that involved Monarch Aviation at its accounts at SCB in Singapore. Dozens of those transactions post-date Woodford and Wang-Woodford's 2003 indictment.

933. Standard Chartered Bank's financing of MODAFL's clandestine and illegal acquisition of U.S. military spare parts through Monarch Aviation did not fund or facilitate Iran's legitimate agencies, operations, or programs. Rather, Standard Chartered Bank actively participated in a criminal conspiracy to help Iran's military and terror apparatus obtain critical machinery and (aircraft) spare parts it desperately needed to sustain its violent and unlawful activities.

[56] SCB, Bahrain's Offshore Booking Unit sent proceeds of the Eurodollar loan as payment of Letter of Credit through SCB's New York branch to credit SCB London's USD account in New York for further payment to SCB Singapore.

[57] SCB, Singapore presented documents under Bank Refah Letter of Credit to SCB, Dubai (the Negotiating Bank) for negotiation and payment in USD funds through SCB's New York branch.

(D) SCB's Trade Finance Transactions with MODAFL-IAIO Front Company Jetpower Industrial Ltd (Hong Kong)

934. Jetpower Industrial Ltd ("Jetpower") was a Hong-Kong based Iranian front company purporting to be a trading company in aircraft parts controlled by Hok Shek Chan, a/k/a John Chan.

935. In 2011, Chan was sentenced to 42 months for conspiring to illegally export, and attempting to illegally export, 10 indicators, used in C-130 military flight simulators, in violation of the Arms Export Control Act.

936. According to the U.S. Department of Justice:

> In 1993, Chan's company, Jetpower Industrial, was convicted in Hong Kong of export violations related to his export of U.S. military parts to Iran. Chan then changed his business practices to avoid detection. Rather than shipping U.S. origin goods directly from Hong Kong to Iran, Chan set up a sophisticated procurement network involving front companies and an experienced freight forwarder in Malaysia. Using his network, the defendant was engaged in the illegal procurement and export of aircraft parts from the U.S. for customers located in Iran, including several military related entities in Iran such as the Iranian Air Force, in direct violation of the U.S. Embargo against Iran since 1997.

937. In fact, according to U.S. officials, Jetpower repeatedly and illicitly exported arms to Iran prior to Mr. Chan's arrest and conviction.[58]

938. At all relevant times, Jetpower was a customer of Bank Melli in Hong Kong.

939. The full scope of Standard Chartered Bank's involvement with and facilitation of Jetpower was extensive (involving at least dozens of transactions) but not yet fully known.

940. Illegal payments totaling close to $3 million dollars have specifically been identified, but the totals could be much higher.

---

[58] At least one Jetpower shipment was seized by UAE officials in 2007 along with several other containers that U.S. officials feared might contain parts or materials that could be used in manufacturing IEDs and EFPs. Bank Mellat financed the transaction, and—according to the LC supporting documentation—the goods were consigned to HESA.

941. What is clear is that Standard Chartered Bank repeatedly and knowingly facilitated the illegal shipment of U.S. origin aircraft parts sold by Jetpower to one of MODAFL's sub-agencies (IHSRC), and that Jetpower was a significant link in Iran's illegal weapons procurement chain.

942. For example, in 2001-2002, Bank Refah (the Issuing Bank) issued a LC to MODAFL's sub-agency IHSRC that was to be reimbursed by Bank Saderat Plc (known then as Iran Overseas Investment Bank), then amended the LC to be available with SCB-Dubai. Standard Chartered Bank's branches in New York, Singapore and Hong Kong were all instrumental in enabling Jetpower's receipt of payments at its Eurodollar account(s) with Bank Melli in Hong Kong.

943. When Jetpower transported the contraband goods (U.S. helicopter parts) to MODAFL (using Iran Air), it asked Bank Melli in Hong Kong to present the documents required under the LC for payment to Standard Chartered Bank Dubai.

944. However, in many instances, Standard Chartered Bank Dubai took at least four extra steps before Bank Melli in Hong Kong received the Eurodollar payment for Jetpower.

945. Upon acceptance of the documents from Bank Melli, Standard Chartered Bank Dubai used the CBI's Eurodollar credit facility with Standard Chartered Bank Dubai and sent instructions for a Eurodollar loan to be issued by Standard Chartered Bank, Bahrain.

946. Standard Chartered Bank, Bahrain booked the loan and sent the proceeds in USD funds as payment under the Letter of Credit through Standard Chartered Bank's New York branch to National Westminster Bank's New York correspondent account for further credit to National Westminster, London for the Eurodollar account of its customer, Bank Melli, London.

947. Standard Chartered Bank, Dubai then sent instructions to Bank Melli, London to pay Bank Melli, Hong Kong upon receipt of USD funds.

948. Variations on this process were undertaken on multiple LCs in USD funds for the benefit of MODAFL's sub-agency.

949. In these cases, Standard Chartered Bank, Bahrain knowingly cleared U.S. dollars through Standard Chartered's New York branch for the illegal trade-finance transactions by repackaging the payments on the LCs as loans that secretly routed through the U.S. to Bank Melli Iran through various British banks.

950. Jetpower, in most cases, ultimately received payment in USD funds to its Eurodollar bank account with Bank Melli Plc's branch in Hong Kong for these illicit transactions with IHSRC.

951. According to BIS-Basel and the Hong Kong Monetary Authority ("HKMA"),[59] all USD transfers from SCB-Hong Kong to Jetpower's account with Bank Melli Plc's Hong Kong branch were cleared by the Hong Kong Clearing House Automated Transfer System and settled by HSBC's Hong Kong subsidiary.

952. None of this illegal conduct was undertaken for the benefit of a legitimate agency, operation or program of Iran.

c. SCB's Trade-Finance Transactions Iran Power Development Company ("IPDC"), MAPNA and Zener Electronics Services (an Agent of Hezbollah)

953. The Iran Power Development Company ("IPDC"), an Iranian government-controlled entity, has worked extensively for years with a network of Iranian companies known as

[59] HKMA is the *de facto* central bank of Hong Kong.

the Mapna Group.[60]

954. Mapna International FZE is a UAE-based subsidiary. One of its directors, Mousa Refan, previously served as the first commander of the Air Force of the "Army of the Guardians of the Islamic Revolution [IRGC]."[61]

955. Another director, Afshin Rezaei, pled guilty in the U.S. District Court for the Northern District of Georgia on April 24, 2008, to:

> one count of violating the IEEPA for the unlicensed export of computers to Iran via the United Arab Emirates. The computers were controlled for anti-terrorism reasons. On May 15, 2008, Rezaei was sentenced to six months of prison (credit for time served), followed by three years of supervised release, and agreed to forfeit $50,000. On February 18, 2010, a 10-year denial of export privileges was imposed on Rezaei, pursuant to Section 11(h) of the EAA.

956. During the relevant time period, Mapna International maintained a Eurodollar account with Standard Chartered Bank, Dubai.[62]

957. Between 2001 and 2007, Standard Chartered Bank facilitated at least 280 Letters of Credit involving Mapna International FZE (as Beneficiary). In most cases, SCB, Dubai acted as the Advising Bank on these transactions.

958. At least nine Letters of Credit involved Standard Chartered Bank's New York branch serving as the Clearing Bank for the transactions, and in some cases, SCB-London served as the Reimbursing Bank.

---

[60] The Mapna Group lists on its website 41 subsidiaries, some of which were listed by the British government in 2011 as entities of concern for Weapons of Mass Destruction-related procurement.

[61] As noted above, Abbas Aliaabadi, Mapna International FZE's chairman, is a former member of the Iranian Ministry of Construction Jihad and of the Iranian Air Force and former member of the Ministry of Culture & Islamic Guidance, instrumental in the creation of Hezbollah and closely linked to the IRGC.

[62] Mapna's subsidiary, Mobin Petrochemicals, was added to the SDN list on June 16, 2010 (and removed from the SDN list in January 2016 as part of the Joint Comprehensive Plan of Action). During the relevant time period, it maintained a USD account with HSBC.

959. Standard Chartered Bank facilitated at least 7 LCs – totaling $1,384,972 in USD funds – that involved the illegal shipment of U.S. origin goods to the Iran Power Development Company.

960. The CBI served as the Issuing Bank on several of these LCs, and six of those seven involved goods shipped by IRISL.

961. Of particular note, between 2003 and 2004, Standard Chartered Bank knowingly facilitated at least four unlawful USD funds transfer transactions (cleared through its New York branch) that involved Eurodollar payments to Zener Electronics (UAE), a procurement company for Hezbollah.[63]

962. The IPDC was listed as the Applicant for these transactions, and Mapna was identified as the 1st Beneficiary, but assigned the payments under the Letters of Credit to Zener Electronics (UAE) as a "2nd Beneficiary."

963. Each unlawful trade-finance transaction involved U.S. goods.

964. The Central Bank of Iran acted as the Issuing Bank on at least two of the transactions and SCB, Dubai acted as the Advising and Negotiating Bank.[64]

965. On at least one occasion, SCB-London served as the Reimbursing Bank for the payment to Zener Electronics, sending the credit through its New York branch to SCB Dubai's account with Standard Chartered Bank in New York.

---

[63] In June 2014, the U.S. Commerce Department identified Zener Electronics as "involved in activities contrary to the national security and foreign policy interests of the United States, specifically the activities described under paragraph (b)(1) (Supporting persons engaged in acts of terror) of § 744.11 of the EAR" and noted its attempts "to procure U.S. technology on behalf of persons involved in activities contrary to the national security and foreign policy interests of the United States. Specifically, these persons have been involved in supplying U.S.-origin items to persons designated by the Secretary of State as Foreign Terrorist Organizations without the required authorizations."

[64] On at least one occasion, SCB London also served as the Reimbursing Bank.

966. Upon receipt of the funds to its USD account with SCB in New York, Standard Chartered Bank, Dubai instructed Standard Chartered Bank's New York branch to forward the funds to JP Morgan Chase in New York, which held an account for the Commercial Bank of Dubai.

967. The Commercial Bank of Dubai, in turn, credited the account of its customer, Zener Electronics.

968. These illicit transfers on behalf of Mapna resulted in payments to Zener Electronics (a key link in Hezbollah's illicit supply chain) and were not for the benefit of a legitimate agency, operation or program of Iran. In a Superseding Indictment filed in federal court on March 30, 2016, Mapna was again implicated in the Conspiracy.[65]

969. This time, DOJ charged multiple individuals with covert transactions in 2011 through a U.S. bank, wherein Mapna's name was omitted from the transaction to hide its identity as a counterparty.

d. SCB's Trade-Finance Transactions with National Iranian Oil Company (NIOC) Subsidiaries

970. The Iranian Helicopter Aviation Company, Ahwaz Pipe Mill Co. and Kala Naft[66] are all subsidiaries of NIOC, which (as noted *supra*) was controlled by, and an agent of, the IRGC during the relevant time period.

971. Between 1999 and 2001, Standard Chartered Bank knowingly facilitated two illegal transactions totaling $750,744 on behalf of the Iranian Helicopter Aviation Company (listed as the Applicant).

---

65 *See*, *U.S. v. Zarrab* filed in the S.D.N.Y (1:15-cr-00867).

66 Kala Naft was designated by the United States in 2010.

972. The Beneficiary listed on both LCs was Limo Sarl. The goods involved in these transactions were U.S. origin helicopter parts.

973. Payments for both transactions were cleared through Standard Chartered Bank's New York branch, and refinanced under the CBI's Eurodollar credit facility with Standard Chartered Bank, Dubai.

974. The Paris-based Limo Sarl was directed by a Ms. Laleh Moein, reported to have also been in the employ of Iran's Ministry of Intelligence and Security ("MOIS").[67]

975. Between 2002 and 2004, SCB knowingly facilitated four (4) illegal transactions totaling $611,713 that involved U.S. origin goods illegally transported to Iran on behalf of Kala Naft.

976. At least two of these transactions had Standard Chartered Bank New York's branch serving as its Clearing Bank.

977. As early as February 1998, Kala Naft was identified by the UK government "as having procured goods and/or technology for weapons of mass destruction programs."

978. Kala Naft was also publicly identified as a NIOC subsidiary in a 2003 Commerce Department action that further stated that Kala Naft was a recipient of illegally exported U.S. origin oilfield equipment from the U.S.

979. Between 2001 and 2006, SCB knowingly facilitated at least two illegal transactions totaling $593,307 that involved U.S. origin goods illegally transported to Iran on behalf of Ahwaz Pipe Mill Co.

980. The CBI was used as the Refinancing Bank, and Standard Chartered Bank's New York branch served as the Clearing Bank.

---

[67] MOIS was designated by the U.S. for, *inter alia*, providing support to terrorist groups, including Hezbollah.

981. The listed beneficiary of the Ahwaz Pipe Mill Co. trade-finance transactions was a Cypriot company named Polygon Co. Ltd.

982. Polygon's managing director and its owner had previously been indicted on November 19, 1992, in the Southern District of Florida for illegally conspiring to export oil field equipment and other goods, services and technology to Libya, demonstrating its history of illicit sanctions evasion on behalf of a State Sponsor of Terrorism.

983. The litany of trade-finance and Eurodollar transactions discussed *supra* often involved counterparties (such as Mac Aviation, Jetpower and Polygon) with established track records of criminal activity on behalf of Iran.

e. SCB's Trade-Finance Transactions with Iranian Front Company Khoram Sanat Producing Co. - Iran

984. On June 20, 2005, Standard Chartered Bank facilitated Khoram Sanat Producing Co.'s purchase of electromotors for hydraulic presses worth $2.79 million.

985. The company is likely a subsidiary of another Iranian company known as "Alborz Steel."

986. The nominal purchaser of the equipment was an Iranian front company in the UAE called Diamonds Steel.[68]

987. Diamonds Steel maintained one or more accounts with Standard Chartered Bank, Dubai.

988. Between 2001 and 2007, SCB, Dubai facilitated at least 173 transactions involving Diamonds Steel, totaling more than $130 million.

[68] SCB facilitated at least a dozen transactions on behalf of Diamonds Steel, mostly for the benefit of Alborz Steel, Iran. Many of these transactions involved both Bank Melli Iran, as well as Credit Suisse in Switzerland, acting on behalf of Bank Melli Iran or Bank Melli, Dubai.

989. The aforementioned electromotors were illegally purchased from the United States with the LC facilitated by Standard Chartered Bank's New York branch, which served as the Clearing Bank for the transaction, while SCB, Dubai served as the Advising Bank.[69]

990. Standard Chartered Bank facilitated this transaction despite the fact that the machinery required an export license because the equipment could be used for terrorist purposes.[70]

991. Specifically, hydraulic presses are the precise type of machinery required to manufacture EFPs.[71]

992. The production of an EFP shaped-charge munition requires at least a 10-ton hydraulic press in order to form sheets of copper and steel, respectively, into the necessary shaped-charge geometry for defeating the plating of American armored vehicles of the type used by the U.S. military in Iraq.

993. Even assuming a steep mark-up in costs of delivery, Standard Chartered Bank financed Iran's acquisition of approximately fifty (50) hydraulic presses capable of manufacturing more than a hundred EFPs per day.[72]

994. The hydraulic press machinery was transported to Iran by IRISL.

---

[69] This occurred during a period of time (between 2004 and 2007) when SCB's New York branch was subject to a formal supervisory action by the New York State Banking Department and the Federal Reserve Bank of New York ("FRBNY") for other regulatory compliance failures involving the Bank Secrecy Act (BSA"), anti-money laundering policies and procedures ("AML"), and OFAC regulations.

[70] The product was designated with an ECCN of 2B999 (for Anti-Terrorism reasons) under Supplement 1 to Section 774 of the Commerce Control List (CCL).

[71] SCB facilitated another Letter of Credit on May 12, 2005, involving Khoram Sanat (as Applicant) and Diamonds Steel (as Beneficiary) for over $1.9 million for goods described as "Back Up Roll Change Carriage, Spare Back Up Roll with Chuck and Main Gear Box." These standard terms are used to describe metal working equipment that may be integrated into large hydraulic presses or deployed as stand-alone equipment stations.

[72] The dangers of Iran possessing hydraulic press equipment were evident from a 2009 reported incident wherein Turkish authorities, at the request of the U.S., halted a convoy of trucks heading from Iran to Syria that contained a large hydraulic press and punch press. The U.S. requested this action because "these items are likely intended for the production of explosively formed penetrators (EFPs)."

995. Because Letters of Credit intrinsically require the submission of detailed paperwork and required Standard Chartered Bank (Credit Suisse and other Defendants) to examine and retain the documentation evidencing Iran's illegal procurement chain, Standard Chartered Bank's knowledge of its role in the Conspiracy is indisputable.

996. Furthermore, because Iran's illegal procurement chain was dependent on access to U.S. dollars, Standard Chartered Bank's (and other Defendants') participation in the Conspiracy was essential to its success.

997. In sum, Standard Chartered Bank was integral to Iran's inherently lethal and illegal conduct, which included a wide variety of money laundering techniques in the service of weapons procurement, arms shipments, acquisition of WMDs, and terror financing that substantially and foreseeably assisted MODAFL, the IRGC and Hezbollah in their campaign of violence and terror against Coalition Forces in Iraq.

3. Regulatory Actions and Criminal Investigations Against Standard Chartered Bank, 2012 – Present

998. On September 21, 2012, Standard Chartered Bank and the New York State's Department of Financial Services ("DFS") executed a Consent Order resolving charges that, from at least 2001 through 2007, Standard Chartered Bank provided Eurodollar clearing and settlement services to Iranian customers subject to U.S. economic sanctions, with respect to approximately 59,000 transactions totaling approximately $250 billion, through Standard Chartered's New York branch.

999. DFS concluded that "SCB operated as a rogue institution."

1000. On December 10, 2012, DOJ announced that SCB had agreed to forfeit $227 million to the Justice Department for conspiring to violate the IEEPA, and that the forfeiture was part of Deferred Prosecution Agreements SCB entered into with DOJ and the Manhattan District

Attorney's office for illegally moving millions of dollars through the U.S. financial system on behalf of, *inter alia*, sanctioned Iranian entities. SCB also entered into settlement agreements with OFAC and the Board of Governors of the Federal Reserve System, as well as with DFS.

1001. DOJ filed a criminal information charging SCB with one count of knowingly and willfully conspiring to violate IEEPA. SCB waived the federal indictment, agreed to the filing of the information and, according to DOJ's press release, "accepted responsibility for its criminal conduct and that of its employees."

1002. DOJ's 2012 press release announcing the Deferred Prosecution Agreement quoted then-Assistant Attorney General Lanny Bruer as stating: "[f]or years, Standard Chartered Bank deliberately violated U.S. laws governing transactions involving Sudan, Iran, and other countries subject to U.S. sanctions. The United States expects a minimum standard of behavior from all financial institutions that enjoy the benefits of the U.S. financial system. Standard Chartered Bank's conduct was flagrant and unacceptable. Together with the Treasury Department and our state and local partners, we will continue our unrelenting efforts to hold accountable financial institutions that intentionally mislead regulators to do business with sanctioned countries."

1003. Manhattan District Attorney Cyrus Vance Jr. stated in the press release: "Investigations of financial institutions, businesses, and individuals who violate U.S. sanctions by misusing banks in New York are vitally important to national security and the integrity of our banking system. Banks occupy positions of trust. It is a bedrock principle that they must deal honestly with their regulators. I will accept nothing less; too much is at stake for the people of New York and this country. These cases give teeth to sanctions enforcement, send a strong message about the need for transparency in international banking, and ultimately contribute to the fight against money laundering and terror financing."

1004. Prior to entering into the 2012 DPA and its settlement with DFS, Standard Chartered Bank retained Promontory Financial Group, LLC ("Promontory") in 2009 to provide "consulting services in connection with the identification and collection of historical transaction records relating to cross-border financial transactions."

1005. In the first half of 2010, Standard Chartered Bank reported to various regulators, including the New York State Banking Department ("NYSBD"), DFS's predecessor, that it had engaged in conduct related to the evasion of U.S. sanctions.

1006. On April 15, 2010, Standard Chartered hired Promontory again to identify, collect and review historical transaction records implicating sanctions violations.

1007. Thereafter, Promontory produced a number of reports and made various presentations to government authorities, including the NYSBD (later DFS).

1008. These Promontory reports included, *inter alia*, interim reports throughout 2010, final reports in January and March of 2011, as well as updates to those final reports in October 2011.

1009. DFS relied in part upon the work conducted and presented by Promontory to identify the scope of Standard Chartered Bank's improper conduct prior to entering into the September 21, 2012 Consent Order.

1010. On June 18, 2013, Deloitte entered into a Settlement Agreement with DFS wherein it agreed, *inter alia*, to pay a penalty of $10 million for misusing confidential information from other bank defendants.

1011. For example, Deloitte provided Standard Chartered Bank with copies of transaction review reports that Deloitte had prepared for these other clients and suggested to SCB management that they be used as templates for SCB's transactions review report, and agreeing to Standard

Chartered Bank's request that Deloitte remove a recommendation from its written final report explaining how "cover payment" messages used by SWIFT-NET (MT 202s) could be manipulated by banks to evade U.S. money laundering controls.

1012. On August 19, 2014, DFS announced an order regarding Standard Chartered Bank's failures to remediate AML/CFT compliance problems as required in Standard Chartered Bank's 2012 settlement with DFS.

1013. Under the August 2014 DFS order, Standard Chartered Bank was required to: (1) suspend dollar clearing through Standard Chartered Bank's New York branch for high-risk retail business clients at SCB's Hong Kong subsidiary; (2) exit high-risk client relationships within certain business lines at SCB's branches in the UAE; (3) decline new dollar-clearing clients or accounts across its operations without prior approval from DFS; (4) pay a $300 million penalty; and (5) take other remedial steps.

1014. Additionally, according to an October 29, 2014 article in *The New York Times*, federal and Manhattan prosecutors reopened their investigation into Standard Chartered Bank.

1015. *The New York Times* reported that prosecutors were questioning whether Standard Chartered Bank failed to disclose the extent of its wrongdoing to the government, thus imperiling SCB's 2012 settlement.

1016. In August 2015, DFS issued a "Report on Investigation of Promontory Financial Group, LLC."

1017. The DFS report stated that:

> On April 15, 2010, Promontory was engaged by Standard Chartered's counsel to identify, collect and review historical transaction records "with certain countries or certain Specially Designated Nationals ("SDNs") subject to sanctions" administered by OFAC. The engagement was known as Project Green.

> As part of the engagement, Promontory produced a number of reports and made various presentations to the Bank and government authorities, including the NYSBD. These reports included interim reports throughout 2010, final reports in January and March of 2011, and updates to those final reports in October 2011.
>
> In connection with the Department's investigation of Standard Chartered, the Department relied in part upon the work conducted and presented by Promontory to identify the scope of the Bank's improper conduct and to determine an appropriate resolution of the investigation.

1018. DFS ultimately concluded that "There are numerous instances where Promontory, at the direction of the Bank or its counsel, or at its own initiative, made changes to 'soften' and 'tone down' the language used in its reports, avoid additional questions from regulators, omit red flag terms or otherwise make the reports more favorable to the Bank."

1019. Examples identified by DFS included a written communication on January 19, 2011, wherein "the Bank's counsel wrote to Promontory that the title of a particular slide entitled 'The 77 non-u-turn payments fell into 3 categories' – meaning the transactions were potential OFAC violations – should be made 'more bland' and suggested a rewording to 'Categories identified in Amendment Analysis.' Promontory made the change to the more vague language requested by the Bank."

1020. The DFS Report further found that "Promontory omitted certain timelines from the reports that would have indicated an increase in violations over time."

1021. The Report went on to cite a December 17, 2010 statement by a senior analyst at Promontory explaining:

> Generally, the timelines serve a strong purpose with the Jersey payments. That is, there appears to be a positive trend over time to reduce the involvement with potential violations. **This will not be true with Dubai. I have a strong suspicion that people will not want to show the timelines for Dubai ([a particular client for which the Bank processed prohibited transactions] for example shows an upwardly sloping curve of violations).** If we are going to go ahead with the visuals across the

> workstreams, we should be cognizant of the graphics showing painful information and expect strong pushback from the bank and [the Bank's counsel]. (Emphasis added.)

1022. As described above, Standard Chartered Bank's Dubai operations were a central hub for the IRGC's and MODAFL's illegal procurement efforts.

1023. In August 2015, *The New York Times* reported that SCB was once again under investigation: "The Justice Department is examining whether it committed sanctions violations beyond those covered in the 2012 deal, which centered on what the bank called 'Project Gazelle,' an effort to forge 'new relationships with Iranian companies.'"

1024. The *Financial Times* also reported in September 2015:

> Documents seen by the FT suggest that StanChart continued to seek new business from Iranian and Iran-connected companies after it had committed in 2007 to stop working with such clients. These activities include foreign exchange transactions that, people familiar with StanChart operations say, would have involved the US dollar….
>
> The material reviewed by the FT depicts a bank — one of the few foreign lenders with a license [sic] to operate in the country — determined to keep working with Iranian companies. The status of numerous Iranian and Iran-connected entities was still being reviewed by StanChart as late as 2013, according to documents seen by the FT. These included entities that had internal "markers" and "blocks" placed against them, a way for the bank to flag up concern about links to Tehran. Many accounts belonging to Iranian or Iran-connected entities were indeed closed by 2007, as StanChart promised. But some, like Bank Saderat — which had sanctions imposed in 2006, or Bank Sepah — still had open accounts with no markers against them.

1025. Even as edited to be favorable to Standard Chartered Bank, the 2011 Promontory Report (attached as Exhibit A to the Amended Complaint) provides a window into the vast array of wrongdoings undertaken by Standard Chartered Bank in concert with Iran and its agents.[73]

[73] Other Promontory reports that have not (for the time being) been publicly disclosed, detail Standard Chartered Bank's Dubai operations and SCB's activities on behalf of the CBI, as well as its role in financing, *inter alia*, Blue Sky Aviation's acquisitions of various materials and technologies.

1026. As the Negotiating Bank on numerous illegal Iranian Letters of Credit, Standard Chartered Bank received the detailed documentation for the shipment of goods and knew that it was helping Iran's military and terrorist apparatus acquire prohibited U.S. goods and dual-use technologies.

1027. In sum, as the Negotiating Bank on numerous illegal Iranian transactions for Mahan Air and various MODAFL sub-agencies, and as an active conduit and money-launderer for the CBI and other sanctioned Iranian banks, Standard Chartered Bank knew that: (1) it was dealing with Iran's military and terrorist apparatus; (2) it was conspiring to evade U.S. export sanctions; (3) it was laundering money in USD funds for Iran's military and terrorist apparatus; (4) its own customers were front companies for Iran's military and terrorist apparatus; (5) these customers were actively engaged in sanctions evasion and money laundering; and (6) none of this illegal conduct was undertaken for the benefit of a legitimate agency, operation or program of Iran.

1028. On April 9, 2019, Standard Chartered Bank entered into yet another Consent Order with DFS agreeing to pay an additional $180 million to address its newly discovered misconduct.

1029. DFS ultimately concluded that "during the period November 2008 through July 2014, the Bank processed nearly 15,000 illegal payments for the benefit of sanctioned Iranian parties, totaling more than $600 million."[74]

1030. These 15,000 illegal payments for the benefit of sanctioned Iranian parties came *after* the U.S. Treasury Department revoked the U-Turn exemption and placed every financial institution in the world on formal notice that Iran and Iranian banks had exploited the U-turn" license to provide "support to terrorist groups."

[74] The factual findings contained in the April 9, 2019 DFS Consent Order are incorporated herein by reference.

1031. Lastly, Standard Chartered Bank chose to use its presence in the United States (and its New York branch specifically) to effectuate its crimes.

L. DEFENDANT ROYAL BANK OF SCOTLAND N.V.'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

1032. As alleged above, Defendant RBS N.V. is the legal successor to ABN Amro Bank. As noted above, this Defendant is referred to herein as "ABN Amro (RBS N.V.)"

1033. In May 1995, top officials of ABN Amro (RBS N.V.) in Amsterdam e-mailed the entire management of ABN Amro (RBS N.V.) in Europe, Asia, South America, Africa, the Caribbean, and North America, advising them that any financial transactions in USD funds undertaken for or on behalf of Iranian persons or banks were subject to seizure or blocking in the United States.

1034. Soon after President Clinton signed the Executive Order implementing sanctions against Iran in May 1995, Iranian banks sought the services of ABN Amro (RBS N.V.) and other banks in aiding Iran to circumvent U.S. laws.

1035. ABN Amro (RBS N.V.) employees were aware of these requests, discussed them with the other Co-conspirator banks, and thereafter approved of ABN Amro (RBS N.V.) conducting the illegal transactions, contrary to the advice of outside counsel retained by ABN Amro (RBS N.V.) that its involvement in such transactions would potentially violate U.S. law.

1036. From approximately 1995 until in or about 2005, ABN Amro (RBS N.V.) conspired with the Iranian Bank Co-conspirators (including the CBI, Bank Melli Iran and Defendant Bank Saderat Plc) and their agents to conceal evidence of ABN Amro (RBS N.V.)'s financial transactions from the U.S. government, law enforcement, and intelligence agencies, as well as U.S. financial institutions charged with detecting and blocking certain Iranian transactions.

1037. ABN Amro (RBS N.V.) was, at the same time, aware that numerous other non-Iranian financial institutions were engaged in the Conspiracy to conceal evidence of the Iranian Bank Co-conspirators' financial transactions from the U.S. government, law enforcement and intelligence agencies, as well as U.S. financial institutions charged with detecting and blocking certain Iranian transactions.

1038. From approximately 1995 until in or about 2005, ABN Amro (RBS N.V.) furthered the Conspiracy by methodically removing and/or falsifying payment messages on its funds transfer systems to disguise the movement of hundreds of millions of U.S. dollars illegally through the U.S. financial system on behalf of the Iranian Bank Co-conspirators (including Bank Melli Iran).

1039. In furtherance of the Conspiracy, ABN Amro (RBS N.V.) and the Iranian Bank Co-conspirators developed methods by which ABN Amro (RBS N.V.) would format USD payments so that such payments would evade U.S. sanctions and detection by automated filters used by financial institutions in the United States.

1040. When ABN Amro (RBS N.V.) employees received payment messages from the Iranian Bank Co-conspirators that contained certain words that could trigger a U.S. bank's automated OFAC filter software algorithms, ABN Amro (RBS N.V.) would manually alter or amend the messages (i.e. "strip" the transactions) to ensure that the transaction would go undetected when it was cleared and settled by financial institutions in the United States.

1041. ABN Amro (RBS N.V.) thereby caused financial institutions in the United States to process transactions involving the Iranian Bank Co-conspirators that U.S. financial institutions would not otherwise have processed.

1042. Like Standard Chartered Bank, certain offices, branches, and subsidiaries of ABN Amro (RBS N.V.) also altered Letters of Credit and foreign exchange transactions involving USD

funds by replacing the names of the Iranian Bank Co-conspirators (including Bank Melli Iran) on those transactions.

1043. Beginning as early as 1995 and continuing until in or about 2005, ABN Amro (RBS N.V.) undertook various acts in furtherance of the Conspiracy. For example: The Dubai branch of ABN created procedures and guidelines to facilitate the processing of prohibited USD transactions.

1044. For instance, one section of the ABN payment manual entitled "Special Conditions" listed specific instructions on how to effectuate these payments and avoid OFAC filters.

1045. A specific instruction from this manual stated: "Payments by order of Iranian Banks …maintaining accounts with ABN, Dubai are to be handled with extra care to ensure the wordings "Iran" etc. are not mentioned in the payment due to OFAC regulations."

1046. In June 1995, an Iranian Bank Co-conspirator requested of ABN Amro (RBS N.V.) officials in Dubai that ABN Amro (RBS N.V.) act as a conduit for all U.S. dollar transactions for that Iranian bank in Dubai.

1047. The Iranian bank requested that all of its USD funds transfer be routed through, or be issued in the name of, ABN Amro (RBS N.V.) and carry no reference to the fact that these payments were issued on its behalf, and that all of its U.S. dollar receipts would come into ABN Amro (RBS N.V.)'s account.

1048. Thereafter, ABN Amro (RBS N.V.) undertook various specific acts to conceal its actions on Iran's behalf.

1049. ABN Amro (RBS N.V.) instructed the Iranian Bank Co-conspirators to include the code word "SPARE" in their payment messages through the bank so that ABN Amro (RBS N.V.)

could first segregate these messages from normal message payment processing, and then amend the message by removing/altering any potentially problematic text, i.e. any reference to Iran.

1050. The payment message would then be stopped by ABN Amro (RBS N.V.), routed into a special queue, and manually altered to avoid being blocked by any OFAC sanctions screening filters.

1051. In this manner, ABN Amro (RBS N.V.) assisted sanctioned entities, and ensured the processing of transactions by formatting payment order messages so that they would not be rejected or blocked by OFAC filters at financial institutions in the United States.

1052. ABN Amro (RBS N.V.) added to its payment manuals the "Special Conditions" that were to be used on behalf of the Iranian Bank Co-conspirators in order to evade detection and circumvent the laws of the United States.

1053. ABN Amro (RBS N.V.) used these same or materially similar procedures with respect to Letters of Credit in USD funds, and the processing of USD denominated checks and traveler's checks.

1054. ABN Amro (RBS N.V.) and the Iranian Bank Co-conspirators knew and discussed the fact that without such alterations, amendments, and code words, the automated OFAC filters at clearing banks in the United States would likely halt most of the payment messages and other transactions, and, in many cases, would reject or block the sanctions-related transactions and report same to OFAC.

1055. ABN Amro (RBS N.V.) also removed the names, BICs, and any other identifying information of the Iranian Bank Co-conspirators in the payment order messages sent to ABN Amro (RBS N.V.)'s U.S. correspondent banks.

1056. In order to circumvent U.S. sanctions, certain Iranian Bank Co-conspirators requested that ABN Amro (RBS N.V.) omit their names and BICs from payment order messages sent by ABN Amro (RBS N.V.) to ABN Amro (RBS N.V.)'s U.S. correspondent banks. ABN Amro (RBS N.V.) complied with the requests of these Iranian Bank Co-conspirators and omitted their names and identifiers in order to help bypass the OFAC filtering mechanisms of U.S. financial institutions.

1057. ABN Amro (RBS N.V.) also used SWIFT-NET MT 202 cover payment messages to shield the identities of the Iranian Bank Co-conspirators.

1058. Instead of using serial MT 103 payment messages that require the names and details of counter-parties to transactions, ABN Amro (RBS N.V.) began using MT 202 cover payment messages expressly for the purpose of avoiding revealing the true identity of the ordering customer and beneficiary party for U.S. dollar payments sent through financial institutions in the United States.

1059. The Central Bank of Iran coordinated with ABN Amro (RBS N.V.)'s Central Bank Desk in Amsterdam regarding the procedure to be followed for repayment of USD deposits to their accounts with European Banks in London.

1060. This procedure stipulated that payment order messages sent to U.S. clearing banks for payment of USD funds to the CBI should not contain any reference to the Central Bank of Iran or any other reference relating to Iran.

1061. In or about June and July 1995, officials at ABN Amro (RBS N.V.)'s Amsterdam Headquarters and New York offices were advised by outside U.S. counsel that the proposal by Iranian banks for ABN Amro (RBS N.V.) to serve as a conduit or means to bypass and avoid the sanctions imposed by the United States upon Iran risked breaching U.S. law.

1062. An internal memorandum generated by ABN Amro (RBS N.V.) at the time stated "[t]he fund transfer mechanics proposed by [the first Iranian Bank] are an attempt to circumvent the Iranian trade embargo. Given that violations of the Executive Order and OFAC regulations carry substantial penalties, not to mention the negative publicity, the [first Iranian Bank] proposal must be strictly scrutinized, and ABN Amro must weigh the risks before proceeding with any such transfers."

1063. Also in June 1995, another Iranian Bank Co-conspirator sent a written communication to certain banks in the UAE and the Iranian Bank's correspondent banks instructing those banks to undertake USD funds transfers for the Iranian bank in the name of a European financial institution "WITHOUT MENTIONING OUR BANK'S NAME" to defeat and circumvent the sanctions imposed upon Iran by the United States.

1064. Like the first request, the Iranian Bank Co-conspirator's request was forwarded to officials located in several departments of the Amsterdam Headquarters of ABN Amro (RBS N.V.).

1065. As early as 1997, in an internal strategy paper for the Middle East and Africa region named "Desert Spring," prepared by ABN Amro (RBS N.V.)'s Middle East and Africa Regional Office, ABN Amro (RBS N.V.) described a "product initiative" with "opportunities in LC discounting for Central Bank and Bank Melli, Iran" and "deposit mobilization from Iranian nationals."

1066. On or about February 5, 2000, an official at the Dubai branch of ABN Amro (RBS N.V.) wrote to a Regional Director of one of the Iranian Bank Co-conspirators assuring him that ABN Amro (RBS N.V.) would take care of carrying out the scheme to evade and defeat the U.S. sanctions.

1067. The ABN Amro (RBS N.V.) official's note stated: "[w]e understand the special nature of your US$ transactions and will ensure that all operations departments concerned are properly briefed regarding this, as well."

1068. A July 19, 2003 e-mail written by John Ciccarone, Head of ABN Amro (RBS N.V.)'s USD Payments Product Management at ABN Amro (RBS N.V.)'s New York branch, discussed the use of MT 202 cover payments, stating: "There is no way the payment will get stopped as all NY ever sees is a bank to bank instruction."

1069. In a July 25, 2003 e-mail, John Philbin, Senior Relationship Banker for Iranian Banks, wrote to Ciccarone:

> Surely Iran is the most obvious case in point for these structures. Twenty-four years of US sanctions and OFAC listing and Iran continues to sell oil and gas in USD. And, it imports and pays in USD as well. All of this is clearly done though accounts in Europe and elsewhere. There is a very good case to be made for getting an overall acceptance that when issues are purely US, we should not be a part of it. In fact, we should see it as an opportunity. OFAC is not the Bible for money laundering (e.g. Cuba is prominent on OFAC). It is a tool of broader US policy. We therefore need to distinguish between US foreign policy on the one hand and AML/anti-Terrorism on the other, however much the US administration may wish to insist that the two are closely linked. It is well worth working on a solution for clients who find themselves in this position or who fear (Syria, Saudi Arabia) that they, one day soon might find themselves there.

1070. Also, in 2003, Diane Perrin, a member of ABN Amro (RBS N.V.)'s Group Compliance team at the Defendant's Amsterdam Head Office, stated that "as a European Institution, we do not comply with US Sanctions because those sanctions are politically motivated."

1071. A 2003 memorandum entitled "Proposal for Establishing a Representative Office in Tehran, Iran" drafted by ABN Amro (RBS N.V.)'s Country Representative in the UAE, Jan Willem van den Bosch, similarly stated:

> The Central Bank of Iran is faced with difficulties for USD denominated clearing transactions due to sanctions imposed by the US. The OFAC filter impounds all Iran related payments and receipts in the US. The Swiss and other European Banks have worked out a solution for this**.** The payment instructions are sent directly to the beneficiary's bank and cover payment is made to the beneficiary bank's US Correspondent as inter-bank payments.

1072. Bosch later coordinated the meeting in Dubai between ABN Amro (RBS N.V.)'s Managing Board Member and CFO Tom De Swann and top functionaries of the CBI, including Aziz Farrashi, CBI's Director General.

1073. During the meeting with the CBI's officials, ABN Amro (RBS N.V.) officials discussed the establishment of the Representative Office by ABN Amro (RBS N.V.) in Tehran and further business development, including the acceptance of USD deposits by the CBI's Desk in Amsterdam.

1074. In an April 20, 2004 e-mail, the aforementioned Philbin mentioned the possibility of using a Jersey Special Purpose Vehicle as a way to circumvent OFAC restrictions:

> Mike Louwerens [ABN Amro's Vice President and Senior Analyst of Country Risk Management Department] mentioned this to me today and sent the attached. The structure below is very interesting and could have applicability for the banks in Iran as well. But whether that is the case or not, what is clear is that this structure envisages our making and receiving payments in USD which will clear through AA in New York. And for which Mike Bowman sees no objection. I am sending a second note in which OEM (Maarten Seckel) gives a go ahead based on Bowman's nihil obstat. The Way for our doing significant business with the Iranian banks in cash may yet be clear.

1075. On July 23, 2004, ABN Amro (RBS N.V.) and its New York branch entered into a Written Agreement with the Federal Reserve Banks of New York and Chicago (collectively, the "Reserve Banks") and other regulators that had detected deficiencies at ABN Amro (RBS N.V.)'s New York Branch relating to AML policies, procedures, and practices that included:

> a pattern of previously undisclosed unsafe and unsound practices warranting further enforcement action…. A. ABN AMRO lacked adequate

> risk management and legal review policies and procedures to ensure compliance with applicable U.S. law, and failed to adhere to those policies and procedures that it did have. As a result, one of ABN AMRO's overseas branches was able to develop and implement "special procedures" for certain funds transfers, check clearing operations, and letter of credit transactions that were designed and used to circumvent the compliance systems established by the Branches to ensure compliance with the laws of the U.S. In particular, the "special procedures" circumvented the Branches' systems for ensuring compliance with the regulations issued by the Office of Foreign Assets Control ("OFAC") (31 C.F.R. Chapter V).

1076. U.S. regulators also found that "[p]rior to August 1, 2004, the New York Branch processed wire transfers originated by Bank Melli Iran, a financial institution owned or controlled by the Government of Iran. The payment instructions on the wire transfers had been modified by one of ABN Amro's overseas branches such that any reference to Bank Melli Iran was removed."

1077. U.S. regulators also found that "[p]rior to August 1, 2004, the Branches advised a number of letters of credit issued by Bank Melli Iran. The letters of credit had been reissued by one of ABN Amro's overseas branches such that any reference to Bank Melli Iran was removed."

1078. As DOJ later concluded: "Each year between and including 1996 and 2004, ABN caused ABN's U.S. affiliate to file false, misleading, and inaccurate Annual Reports of Blocked Property to OFAC. In each of those reports, the U.S. affiliate of ABN certified to OFAC that all information provided was accurate and that all material facts in connection with the report had been set forth."

1079. Nonetheless, in September 2004, Michael Louwerens, ABN Amro (RBS N.V.)'s Vice President and Senior Analyst of Country Risk Management Department, travelled to Iran at the behest of ABN Amro (RBS N.V.)'s Head Office and reported back that he had communicated with the Chief Representative of HSBC in Tehran (presumably John Richards) and concluded that ABN Amro (RBS N.V.)'s payment procedures (to conceal Iranian financial activity) were in line with prevailing market practices of HSBC and other banks.

1080. In addition, ABN Amro (RBS N.V.)'s then-New York branch was the conduit for at least 90 post-U.S. designation transactions on behalf of IRISL and its various front companies through March 2010.

1081. On May 10, 2010, DOJ issued a press release announcing that ABN Amro's successor entity, Defendant Royal Bank of Scotland N.V., had agreed to forfeit $500 million to the United States in connection with a conspiracy to defraud the United States, to violate the IEEPA, the TWEA, and the Bank Secrecy Act ("BSA").

1082. In connection with a Deferred Prosecution Agreement ABN Amro (RBS N.V.) entered into, a criminal information was filed in the U.S. District Court for the District of Columbia charging the Defendant with one count of violating the BSA, and one count of conspiracy to defraud the United States and violate the IEEPA and the TWEA. ABN Amro (RBS N.V.) waived indictment, agreed to the filing of the information, and, according to the press release "accepted and acknowledged responsibility for its conduct."

1083. According to the criminal information, ABN Amro (RBS N.V.)'s participation in the conspiracy continued "until in or about December 2007." Prior to that time, ABN Amro (RBS N.V.) willfully and knowingly conspired, *inter alia*, to "engage in financial transactions with entities affiliated with Iran … in violation of the International Emergency Economic Powers Act, Title 50, United States Code, Section 1705, and regulations and embargoes issued thereunder…."

1084. The criminal information confirmed that ABN Amro (RBS N.V.) was an active participant in the Conspiracy.

1085. The criminal information stated that: "It was part of the conspiracy that the defendant discussed with the co-conspirators how to format United States Dollar message

payments so that such payments would avoid detection by automated filters used by financial institutions in the United States and thus evade United States sanctions."

1086. The criminal information further stated that: "It was part of the conspiracy that the defendant removed names and references to the co-conspirators in United States Dollar message payments routed through the United States."

1087. The criminal information further stated that: "It was part of the conspiracy that the defendant altered the names and references to the co-conspirators in United States Dollar message payments routed through the United States."

1088. The criminal information further stated that: "It was part of the conspiracy that the defendant instructed the co-conspirators to use code words in United States Dollar payment messages."

1089. Additionally, the criminal information stated that: "It was part of the conspiracy that the defendant created a special processing queue to manually and materially alter any of the co-conspirators' United States Dollar message payments that were to be routed through the United States."

1090. The criminal information also stated that: "It was part of the conspiracy that the defendant created "Special Conditions" in the defendant's payment manuals in order to process any co-conspirators' United States Dollar transactions."

1091. Finally, the criminal information further stated that: "It was part of the conspiracy that the defendant caused its United States affiliates to submit materially false and misleading reports or statements to the United States Department of the Treasury, OFAC."

M. DEFENDANT CREDIT SUISSE'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

1092. Like the other Defendants in this Action, Credit Suisse worked hand-in-glove with

Iran and Iranian Bank Co-conspirators acting at Iran's behest to develop procedures to structure USD payments in ways that would evade U.S. sanctions and leave U.S. regulators, law enforcement and financial institutions blind as to Iran's financial activities.

1093. To this end, Credit Suisse worked diligently to (1) develop methods that would avoid disclosing the true originators and/or beneficiaries of Iranian transactions that it was clearing and settling in the United States; (2) delete or omit certain information when transactions were to be processed through the United States; and (3) provide incorrect information in USD funds transfer instructions executed through the United States on behalf of U.S.-sanctioned individuals and entities.

1094. Credit Suisse worked closely with Bank Melli, Bank Saderat, and Iran's Atomic Energy Organization (and other designated Weapons of Mass Destruction proliferators) for many years.

1095. Before 2003, Credit Suisse was an active participant in the Conspiracy, but the sheer volume of its illegal conduct accelerated greatly in 2003 when Lloyds exited its Iran business and Bank Melli Plc, Defendant Bank Saderat Plc, and other Iranian agents moved their accounts to Credit Suisse.

1096. For the next two years, Credit Suisse became one of the main USD funds clearing banks for the Iranian banking system, quadrupling in only 3 years the number of Iranian U.S. dollar payments, from approximately 49,000 in 2002 to nearly 200,000 in 2005.

1097. The procedures Credit Suisse developed and refined over time to assist Iran were embodied in internal directives, memoranda, e-mails between Credit Suisse and its Iranian bank clients and internal e-mails involving, among others, a Credit Suisse Bank Payments Sector Head,

Credit Suisse's Treasury and Trade Finance Departments, and the Head of Credit Suisse's Iran Desk.

1098. Since at least the mid-1990s, when it first agreed to assist Iran in carrying out the Conspiracy, Credit Suisse's Iran Desk began adding internal warnings to the accounts of its Iranian bank clients, instructing Credit Suisse employees: "*Do not mention the name of the Iranian bank in payment orders*."

1099. Such warnings ensured that payment orders given by the Iranian Bank Co-conspirators would not be processed automatically, but rather would be manually reviewed, "corrected" if necessary, and effectuated by Credit Suisse employees.

1100. For example, in June 1995, the Credit Suisse representative office in Dubai, United Arab Emirates, issued a memorandum recognizing Iran and the Iranian bank's general scheme to ensure that *any* foreign banks the Iranian Bank Co-conspirators did business with masked their transactions, and accordingly advised:

> Following the decision by the American authorities to declare a unilateral embargo against the Islamic Republic of Iran on April 30th, (an Iranian bank) approached Credit Suisse to open (a type of correspondent banking account for U.S. dollar transactions). Crucial to them was that the name of the bank would not be mentioned on the transfer orders... Subsequently, (the Iranian bank) was informed that though payments in such a way are basically feasible, to omit the name of the bank could lead to some problems. Meanwhile, operations through this account have started... Some transfers have been rejected by the American banks as the name of (the Iranian bank) appears under the rubric 'Ordering Bank.' Question: a) what can be done to avoid this?

1101. Almost immediately after President Clinton issued E.O. Nos. 12957, 12959, and 13059, which strengthened existing U.S. sanctions against Iran, the Iranian Bank Co-conspirators began requesting that Credit Suisse omit their names and BICs from payment messages Credit Suisse sent to its U.S. correspondent banks.

1102. Credit Suisse complied with the Iranian Bank Co-conspirators' illegal requests and purposefully omitted their names and identifiers in order to help bypass U.S. financial institutions' sanctions filters.

1103. After a 1998 corporate reorganization, in order to further its ongoing efforts to evade U.S. sanctions and ensure that other U.S. financial institutions would automatically process this new stream of payments, Credit Suisse notified its Iranian clients about the change in USD funds clearing and settlement from Credit Suisse First Boston AG ("CSFB") to third-party U.S. correspondents, and provided them with a pamphlet entitled "How to transfer USD payments."

1104. The pamphlet provided detailed payment order formatting instructions for USD funds transfers on how to avoid triggering U.S. OFAC sanction screening filters.

1105. In a 1998 letter to an Iranian Bank Co-conspirator explaining the transfer of its USD clearing services to the Bank of New York, New York, Defendant Credit Suisse wrote:

> In order to provide your esteemed institution with our clearing services in U.S. Dollars, we have introduced a procedure to facilitate your USD payments through our clearing system. The change of our USD-clearer to Bank of New York, New York, will not affect our mutual relationship on any clearing transaction in U.S. Dollars as long as the established procedure will be followed.

1106. Beginning as early as 1995 and continuing through 2005, Credit Suisse, both internally and in coordination with the Iranian Bank Co-conspirators, created procedures and guidelines to facilitate the processing of prohibited USD transactions by its U.S. correspondent banks, primarily the Bank of New York, New York.

1107. By using Credit Suisse's internal processing system, employees manually keyed in "Order of a Customer" when Iranian payments had to be processed as serial payments through U.S. banks.

1108. This procedure was promoted at Credit Suisse, as demonstrated by an email from a Team Leader in the Bank Payments Unit:

> In order to put an end, once and for all, to the discussions regarding the processing of USD payment orders of Iranian banks, I have worked out various examples that are to be considered binding for everyone.

1109. Attached to the email were several screenshots of Credit Suisse's payment application illustrating how to format payment order messages to ensure that they would pass through the U.S. financial institutions undetected by U.S. OFAC sanction screening filters.

1110. For example, one such screenshot showed all incoming payment messages listing an Iranian bank as the ordering institution in SWIFT-NET payment order message field "52" and contained the following explicit instructions: "Population of field 52 with 'one of our clients' in case of serial payments via the US."

1111. A second screenshot showed an incoming payment with the reference "*without mentioning our banks [sic] name*" in field 52 and contained the following instructions: "Population of field 52 with 'one of our clients' in case of serial payments."

1112. Until 2004, Credit Suisse's use of "*Order of a Customer*" was its standard procedure for processing bank payment messages involving Credit Suisse's Iranian customers.

1113. Credit Suisse's internal communications also reveal a continual dialogue about evading U.S. sanctions spanning approximately a decade, assessing how to better process Iranian transactions in order to promote and increase business from existing and future Iranian clients.

1114. In February 1999, Credit Suisse's Iran Desk added internal warnings to the Customer Information Files (or "CIFs") it maintained for the accounts of its Iranian bank customers, expressly directing Credit Suisse employees: "*Do not mention the name of the Iranian bank in payment orders*."

1115. Credit Suisse documented similar directives in subsequent years. For example, in 2002, another warning was loaded in the CIF that likewise stated: "FOR USD-PAYMENTS OUTSIDE CREDIT SUISSE/CS FIRST BOSTON DO NOT MENTION THE NAME OF THE IRANIAN BANK."

1116. Credit Suisse later decided to remove warnings from the CIFs and replaced them with long-term instructions concerning Iranian entities that instructed: "*Execute USD payment orders always with direct order and cover payment*." These instructions explained that they were intended to ensure (according to Credit Suisse's internal documentation) that "an Iranian origin will never be named in USD payments carried out for Iranian banks (because of the US sanctions)!"

1117. An internal Credit Suisse memorandum dated March 12, 1999, stated:

> Payment orders in USD can only be paid via the American clearing, if the name of the Iranian party is not mentioned (US sanctions). Otherwise, the amounts are returned by the American banks. Even though corresponding warnings have been loaded, there (sic) almost every week cases that are processed incorrectly by us.

1118. Between 2000 and 2004, Credit Suisse's Iran Desk provided similar instructions to its Iranian Bank Co-conspirator clients via a standard letter, which stated in part: "*The most important issue is that you and/or your* correspondents do not mention your good bank's name in field 52."

1119. Credit Suisse's Iran Desk also informed Iranian Bank Co-conspirator clients that Credit Suisse would utilize cover payments to effect payments to or through the United States, stating in one memorandum, for example, "[o]ur payment department will stop all USD payments initiated by your fine bank in any case and shall be effected [by]... 'Direct payment order and cover payment order.'"

1120. In order to prevent straight-through processing of all payment orders sent by Iranian Bank Co-conspirators, Credit Suisse configured its payment system to interdict the payments for manual review.

1121. Credit Suisse employees then reviewed the payments to ensure that they contained no references to Iran. If such references were detected, Credit Suisse employees would either delete the reference, or contact the Iranian Bank Co-conspirators to request further instructions.

1122. Over time, Credit Suisse employees developed practices to omit information on the involvement of Iranian Bank Co-conspirators, including:

a. Entering in an empty field, or replacing the name of the Iranian Bank Co-conspirators with, "*Order of a Customer*" or a similar phrase instead of the actual name of the ordering institution in SWIFT-NET payment order messages;

b. Forwarding payment messages received from Iranian Bank Co-conspirators falsely referencing "Credit Suisse" or Credit Suisse's SWIFT-NET account code (identified by BIC address CRESCHZZ) instead of an Iranian bank as the originating institution. For example, a November 2000 email circulated by a team leader in Credit Suisse's Bank Payments Unit contained screenshots of an incoming payment order from an Iranian bank co-conspirator in which Credit Suisse was listed as the ordering institution in field "52" of the SWIFT-NET payment message. The instructions were to make no changes to the misleading information in the SWIFT-NET message's field "52" for serial payment messages made to U.S. financial institutions;

c. Inserting "Credit Suisse" as the ordering institution in payments originating with an Iranian Bank Co-conspirator;

d. Removing all references to Iranian names, addresses, cities, and telephone numbers from customer payments;

e. Substituting abbreviations for Iranian customer names. For example, in an April 16, 2003 email, the Head of Credit Suisse's Iran Desk wrote to the Credit Suisse representative office in Tehran, "*entry to their account works when account number plus XXX is stipulated as beneficiary. What is also important of course is that*

applicant will give details of final beneficiary as reference for the beneficiary, then it should work;" and

f. Converting SWIFT-NET MT 103 Messages to SWIFT-NET MT 202 Messages to hide the details of Iranian transactions and using MT 202 cover payment messages approximately 95% of the time to facilitate outgoing customer payments involving Iran or Iranian parties.

1123. A September 24, 2003 Credit Suisse internal email sent from a team leader in Customer Payments to a Sector Head within Customer Payments, described Credit Suisse's Iranian U.S. dollar processing:

> The procedure is identical for all Iranian banks: 1) We attempt to send all USD payments directly to the bank of the beneficiary. Only cover payments are made through the US. In such cases, the ordering institution is not disclosed. 2) Should 1) not be possible (if the beneficiary bank is an American bank, or if no Swift connection or no correspondent was named), then the payment will be made though America. We make sure that the ordering institution is not mentioned (this has been programmed into the system as a default) and that the ordering customer has no connection to 'Iran'. 3) Should 1) and 2) not be possible, then the payment order will be forwarded to Investigations for further clarifications with the ordering institution.

1124. In addition, Credit Suisse actually instructed its Iranian Bank Co-conspirator customers on how to format U.S. dollar payments so that such payments would evade U.S. sanctions and detection by automated filters used by U.S. financial institutions.

1125. Payment instructions included a letter from Credit Suisse's Iran Desk to an Iranian customer dated October 16, 2003, that stated: "This is to provide you our recommendation for the entry of funds how to handle bank-to-bank payments on your account with Credit Suisse and the following procedures should be applied in order to avoid any difficulties."

1126. In December 2003, an Iranian bank asked Credit Suisse for an additional USD account identifying the Iranian beneficiary bank only by a designated abbreviation (first letter of

each word constituting the bank's name, together with the abbreviation commonly used for a type of legal entity, i.e., Plc).

1127. On January 28, 2004, Credit Suisse confirmed that it had opened the requested account, writing to the Iranian bank: "Reference is made to the various conversations and your email, dated December 18, 2003 wherein you asked us to open a new USD account...Now, we would like to confirm the account number …."

1128. In addition, Credit Suisse promised the Iranian Bank Co-conspirators, including Bank Saderat and Bank Melli, that no messages would leave Credit Suisse without being first hand-checked by a Credit Suisse employee to ensure that they had been formatted to avoid U.S. OFAC filters.

1129. Credit Suisse also took a further step in the Conspiracy beyond *training* the Iranian Bank Co-conspirators on how to format their payment messages to evade the OFAC filters; it also gave Iranian Bank Co-conspirators materials to use for training *other* banks on how to prepare payment messages to evade U.S. OFAC filters and sanctions regimes.

1130. In August 2003, Credit Suisse reached an agreement with the London branches of a number of Iranian Bank Co-conspirators to take over the banks' London branches' U.S. dollar clearing activity.

1131. As a result of this agreement, Credit Suisse became one of the main USD clearing banks for the Iranian banking system.

1132. Through its subsidiary Credit Suisse Asset Management Limited, United Kingdom ("CSAM"), Credit Suisse used code words for Iranian customers, including Iranian Bank Co-conspirators, when executing trades involving U.S. securities that were transmitted through the U.S.

1133. Credit Suisse knew that without such alterations, amendments, and code words, automated OFAC filters at U.S. clearing banks would likely halt the payment order messages and securities transactions, and, in many cases, reject or block the sanctions-related transactions and report the same to OFAC.

1134. Credit Suisse manipulated payment order messages and removed any identifying reference to sanctioned countries and entities so that the OFAC filters at the U.S. clearing banks would not be able to identify the transactions, and the transactions would be automatically processed without detection.

1135. In July 2004, the Swiss Federal Banking Commission issued an ordinance to implement the Financial Action Task Force ("FATF")'s Special Recommendation on Terrorist Financing VII.

1136. The ordinance required the disclosure of the remitter in payment orders and prompted Credit Suisse to issue an internal directive prohibiting the use of the "Order of a Customer" method when making international wire transfers.

1137. In April 2004, in preparation for the implementation of the ordinance, Credit Suisse's Iran Desk began to inform its Iranian Bank Co-conspirator clients that neither "Order of a Customer" nor "Credit Suisse" could be used to replace references to Iranian banks on payment messages.

1138. Credit Suisse again, however, provided information about the use of the cover payment method to send USD payments, ensuring that the Iranian Bank Co-conspirators (and, by extension, Iran and the IRGC-QF) remained cognizant of other means of ensuring an uninterrupted flow of surreptitious USD.

1139. Although Credit Suisse's payment processing units ceased to use the "Order of a

Customer" method following the Swiss Federal Banking Commission's July 2004 ordinance, Credit Suisse employees nonetheless continued removing and/or altering information in SWIFT payment order messages sent to one of its U.S. correspondent banks.

1140. For example, in May 2005, an internal Credit Suisse email stated:

> If we do not have a key contact with the beneficiary's bank, we have to carry out the payment via the US, e.g. via BKTRUS33. However, no reference to Iran may be made in the field reserved for information on the ordering party (no Iranian telephone numbers either). No such reference should be made in fields 70 or 72 either.

1141. Between March 2004 and November 2005, Credit Suisse repeatedly sent letters to its Iranian Bank Co-Conspirator customers describing its internal procedures for forwarding Iranian payment orders as:

> Our Payment department will stop all USD-payments initiated by your fine bank in any case and shall be effected as outlined in the drawing "Direct payment order and cover payment order."

1142. From August 2003 to November 2006, Credit Suisse illegally processed electronic funds transfers, in the aggregate amount of at least *$480,072,032*, through financial institutions located in the United States for the benefit of Iran and Iranian financial institutions.

1143. For a brief period of time, Credit Suisse became one of the main U.S. dollar clearing and settlement banks for the Iranian banking system.

1144. In January 2006, Credit Suisse established a "Sensitive Countries" Task Force to implement the exit decision and ultimately ceased U.S. dollar clearing transactions for Iran in November 2006.

1145. On September 11, 2006, Credit Suisse directed its payments centers to discontinue certain prohibited payments by an Iranian Bank Co-conspirator. Using the MT 202 cover payment method, during the six weeks from September 11, 2006 to October 27, 2006, Credit Suisse

nevertheless processed 54 outbound payments involving that Iranian Bank Co-conspirator, the total value of which was in excess of $8 million.

1146. As described *supra*, Credit Suisse also facilitated payments on Letters of Credit involving Mahan Air's illegal purchase of U.S. aircraft and aircraft parts.

1147. These included the illegal purchase of an aircraft engine and an Airbus A320-232 financed by Bank Melli, Bank Refah and Bank Sepah.

1148. In each case, Credit Suisse directed USD payments through the United States in furtherance of the Conspiracy.

1149. In March 2007, following the Deferred Prosecution Agreements of Lloyds and ABN Amro (RBS N.V.), Credit Suisse commenced an internal investigation of its historic USD funds clearing business involving U.S.-sanctioned countries and persons. Shortly thereafter, Credit Suisse was contacted by U.S. and New York law enforcement officials.

1150. On December 16, 2009, DOJ issued a press release announcing that Credit Suisse had agreed to forfeit $536 million in USD funds to the United States and to the Manhattan District Attorney's Office in connection with violations of the IEEPA and New York State law, as a result of violations relating to transactions Credit Suisse illegally conducted on behalf of customers from, *inter alia*, Iran.

1151. In connection with a DPA that Credit Suisse entered into, DOJ filed a criminal information in the U.S. District Court for the District of Columbia charging Credit Suisse with one count of violating the IEEPA. Credit Suisse waived the indictment, agreed to the filing of the information, and, according to the press release, accepted and acknowledged responsibility for its criminal conduct.

1152. Credit Suisse also simultaneously entered into an agreement with OFAC to settle

its violations of the IEEPA and agreed to a civil forfeiture as part of the DPA it entered into with DOJ, the Manhattan District Attorney's Office and OFAC.

1153. The press release announcing the agreements quoted then-Treasury Under-Secretary for Terrorism and Financial Intelligence Stuart Levey as stating "[t]his case provides a timely lesson about how Iran seeks to involve others in deceptive conduct to evade legal and regulatory controls. Those who do business with Iran expose themselves to the risk, and the consequences, of participating in transactions supporting proliferation, terrorism or sanctions evasion."

N. DEFENDANT COMMERZBANK AG'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

1154. As noted in a criminal information entered in connection with, as discussed below, a March 11, 2015 Deferred Prosecution Agreement between Defendant Commerzbank and DOJ:

> COMMERZBANK AG and others … unlawfully, willfully and knowingly combined, conspired, confederated and agreed with one another and with others to commit offenses against the United States, that is, to engage in financial transactions with Sanctioned Entities and SDNs in violation of IEEPA, and the executive orders and regulations issued thereunder.… The goal of the conspiracy was for COMMERZBANK and others …to enrich themselves by engaging in a conspiracy and a scheme to violate IEEPA, and the executive orders and regulations issued thereunder. A further goal of the conspiracy was for COMMERZBANK and others … to violate executive orders and regulations prohibiting the exportation, directly and indirectly, of services from the United States to Sanctioned Entities and SDNs.

1155. Like many of the other Defendants who entered into the Conspiracy, Commerzbank adopted a variety of methods to facilitate Iran's illegal goals.

1156. In particular, Commerzbank worked with Bank Sepah, Bank Melli, Bank Saderat and Bank Refah to facilitate the goals of the Conspiracy, stripping, altering or changing tens of thousands of SWIFT-NET payment order messages.

1157. Since 2002, Commerzbank also appears to have engaged in various illegal gold transactions on behalf of the CBI, including trading orders through its New York branch while disguising the Iranian source of the trades.

1158. A March 2015 Amended Complaint filed in a *qui tam* case against Defendant Commerzbank AG stated that:

> the gold trade has been essential to Iran's withstanding the increasingly restrictive U.S. sanctions. It has a substantial amount of gold reserves, amounting to $112 billion in gold, which it accumulated in part by trading oil for gold. It used gold to preserve its wealth especially to withstand the devaluation of its currency and to engage in trading that would bypass U.S. sanctions.[75]

1159. On April 17, 2003, Commerzbank finalized a policy document entitled "Routing Instructions Iranian banks for USD payments." This policy admonished employees to "[u]nder no circumstances mention the Iranian background in the cover order." In other words, the German-based recipients of this policy were instructed to never mention Iranian customers nor Iranian connections to any payment messages sent to the United States.

1160. Taking advantage of the fact that Lloyds and other competitors were exiting the Iran market, Commerzbank solicited more Iranian clients.

1161. The resulting increase in the volume and significance of Iranian business at Commerzbank led to the establishment of a centralized process for handling certain Iranian dollar denominated payments within Commerzbank, and the Defendant designated one group of employees within Commerzbank's Frankfurt Back Office to manually process those payments. The task of this group was to review payments and amend them if necessary, to ensure that they

[75] In July 2015, Commerzbank settled the *qui tam* case, 13-cv-8095 (S.D.N.Y. 2013), for approximately $866,000.

would not get stopped by OFAC filters when sent to financial institutions in the United States, including Commerzbank's New York branch.

1162. This increase in volume was in part due to illicit trade-finance, foreign exchange, and Eurodollar transactions undertaken by Commerzbank on behalf of Bank Refah, Bank Sepah, Bank Melli and Bank Saderat.

1163. In July 2003, a Back Office employee emailed other bank employees explaining that two state-owned Iranian banks, Bank Melli and Bank Saderat, wanted to begin routing their entire USD funds clearing business through Commerzbank. The Back Office employee closed his email by writing, "If for whatever reason [Commerzbank] New York inquires why our turnover has increase [sic] so dramatically under no circumstances may anyone mention that there is a connection to the clearing of Iranian banks!!!!!!!!!!!!" (Exclamation marks in the original).

1164. On September 17, 2003, a Back Office employee sent an email advising a major Iranian Bank that maintained a US dollar account with Commerzbank to list "non ref" in the ordering party field in all of its future payment messages.

1165. The author of the email had tested Commerzbank's compliance systems in Frankfurt, and knew that writing "non ref" would trigger a manual review of the payment, thereby enabling Commerzbank personnel to ensure that the messages did not contain any information revealing the true Iranian involvement in the transaction.

1166. In fact, Commerzbank personnel explained to employees of Iranian bank clients the kinds of information that could lead to payments being delayed, rejected, or blocked within the United States, and encouraged the Iranian banks to omit this type of information from their payment orders so that Commerzbank employees would not have to manually remove it.

1167. For example, Bank Sepah's UK subsidiary (Bank Sepah International Plc) provided its Iranian customers with routing instructions for "payments to our US Dollar account from outside the United States" noting the SWIFT Code for Commerzbank's New York branch and the Bank's account number at Commerzbank followed by the instruction:

> **Please ensure that no mention is made of any recognisable Iranian entity in any message sent through the United States.**

(Emphasis in the original.) *See* Exhibit B attached.

1168. On October 13, 2003, the Head of Commerzbank's Internal Audit division emailed a member of Commerzbank's senior management advising that Iranian bank names in payment messages transiting through the United States were being "neutralized" and warned that "it raises concerns if we consciously reference the suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the U.S.A."

1169. On November 19, 2003, a memo was circulated to senior management memorializing the internal rules Commerzbank had developed for processing Iranian payments, including using MT 202 cover transactions (i.e., splitting a payment into two messages and sending a MT 103 to the foreign (non-U.S.) branch of the beneficiary and an MT 202 to the clearing institution in the United States), and using serial MT 103 messages that manually replaced the name of the (Iranian) ordering party with the bank code for Commerzbank Frankfurt to avoid detection by U.S. authorities.

1170. It appears that Commerzbank may have ceased stripping some transactions in July 2004, relying primarily on cover payments (MT 202 payment order messages) to effectuate its unlawful conduct. At the same time, Commerzbank conspired with Bank Melli to facilitate over one hundred (100) checks totaling approximately $2 million in USD funds that Commerzbank issued for illegal payments in the United States.

1171. However, as noted *supra*, Bank Sepah International Plc (Bank Sepah's UK subsidiary) provided "stripping" instructions to its clients even in 2006 directing that U.S. dollars wire transfers be sent through Commerzbank's New York branch.

1172. DOJ described "the rigor with which the Bank enforced the policy during this period" by citing an email from a Back Office employee who wrote about Commerzbank's procedures for facilitating the Conspiracy "NO EXPERIMENTS PLEASE!!! Have fun with this and greetings." (Emphasis in the original.)

1173. This ongoing conduct involving both "stripping" transactions and converting otherwise transparent SWIFT-NET MT 103 messages into opaque MT 202 cover transactions resulted in tens of millions of dollars being illegally transferred on Iran's behalf.

1174. However, parallel to its illegal conduct on behalf of Bank Sepah, Bank Saderat and Bank Melli, as noted above, Commerzbank also directly coordinated with IRISL in laundering U.S. dollars through the United States despite the fact that IRISL was Iran's primary means of transporting both conventional and non-conventional weapons.

1175. Between 2002 and 2008 (and upon information and belief, even later), Commerzbank worked directly with IRISL to facilitate illicit payments through the United States.

1176. In January 2005, Commerzbank's New York branch rejected a series of payment transactions on behalf of Lancelin Shipping Company Ltd., an IRISL-formed entity registered in Cyprus, because the payment messages contained references to IRISL Europe GmbH, a wholly-owned IRISL subsidiary registered in Hamburg and designated by the United States in 2008.

1177. This prompted a direct meeting between the relationship managers in Commerzbank's Hamburg branch and employees from IRISL on January 24, 2005.

1178. A memorandum summarizing the meeting noted that: "[d]ue to the tense political relations between Iran and the U.S., sanctions that have existed for some years against Iran and Iranian companies have been tightened…. *The number of rejected payments recently increased sharply since the word "IRISL" results in inquiries at foreign banks.* Based on inquiries from Commerzbank, New York we assume that it appears as a term on the embargo list." (Emphasis in the original.)

1179. In a written presentation that Commerzbank delivered to IRISL on January 25, 2005, following the in-person meeting, the Hamburg relationship manager stated: "*[t]he current rejections show that IRISL is in the OFAC list*" (Emphasis in the original).

1180. The presentation then explained that "payments which are sent through a ... subsidiary are unlikely to be rejected to our present knowledge."

1181. Commerzbank ultimately adopted a process it termed a "safe payments solution" by which IRISL initiated USD funds transfers through the U.S., using the accounts of less conspicuous subsidiaries to prevent its New York branch or other clearing banks from flagging IRISL U.S. dollar transactions.

1182. Moreover, to assist IRISL in its bookkeeping, Commerzbank would sweep those accounts daily and zero them out so that IRISL could keep track of which USD funds belonged to it – as opposed to its subsidiaries.

1183. On April 18, 2006, Commerzbank's New York branch rejected a payment on behalf of Lancelin, citing "US sanctions against Iran." As a result, Commerzbank altered the structure of the "safe payment solution," suggesting the use of two other subsidiaries to process payments on behalf of IRISL and IRISL Europe GmbH.

1184. In fact, in only four months *following* IRISL's U.S. designation in 2008, Commerzbank illegally transferred almost $40 million on behalf of IRISL subsidiaries and related entities through Commerzbank's New York branch and other U.S. financial institutions.

1185. These post-designation transactions, laundered by Commerzgank through the U.S. financial system, were self-evidently *not* for the benefit of a legitimate agency, operation or program of Iran.

1186. Only months earlier, a U.S. State Department diplomatic cable warned of an IRISL-flagged vessel in China loaded with cargo containing weapons for Iran's Defense Industries Organization ("DIO").

1187. The 2008 diplomatic cable further warned of the dangers of ongoing conventional arms transfers from China to Iran, "particularly given Iran's clear policy of providing arms and other support to Iraqi insurgents and terrorist groups like the Taliban and Hezbollah…. We have specific information that Chinese weapons and components for weapons transferred to Iran are being used against U.S. and Coalition Forces in Iraq, which is a grave U.S. concern."

1188. Less than a year after Commerzbank in Hamburg provided IRISL with at least $40 million in illegal (post-designation) USD transactions in October 2009, U.S. troops boarded a German-owned freighter, the *Hansa India*, in the Gulf of Suez and found eight containers full of ammunition, and headed to Syria from Iran.

1189. The *Hansa India* was registered to the Hamburg-based shipping company Leonhardt & Blumberg but had in fact been under charter to IRISL for several years.

1190. The *Hansa India* carried seven containers of small arms ammunition, as well as one container containing copper discs, which constitute, as noted *supra*, a key component in EFPs used to kill and maim hundreds of U.S. service members.

1191. Although Commerzbank worked to shield its New York branch from knowing all of the details of its illicit activities on behalf of Iran and IRISL, Commerzbank's New York branch was nonetheless aware that it was being used to facilitate unlawful conduct.

1192. For example, in June 2006, in response to a request from the new Chief Compliance Officer asking if there were any concerns they wanted her to share with the new Global Head of Compliance in Germany, a New York compliance employee responded "[p]ersistent disregarding of OFAC rules by foreign branches. Hamburg is notorious for it."

1193. In February 2007, Commerzbank's then Chief Executive Officer Klaus-Peter Mueller and Board Member Martin Blessing met with U.S. Treasury Deputy Secretary Robert Kimmitt. In the meeting, Mueller complained about the portrayal of Commerzbank by *The Wall Street Journal* (in a January 2007 article) which he said made it appear that the Bank was trying to evade sanctions on Iran. "This," claimed Mueller "is far from the case."

1194. *The Wall Street Journal* reported on January 10, 2007 that "Commerzbank AG, Germany's second largest bank, said it will stop handling dollar transactions for Iran at its New York branch by Jan. 31." It went on to report that "[a]t present, Commerzbank handles both dollar and euro transactions for Iran's state-owned banks. Like several other European banks, it will cease handling only dollar transactions."

1195. *The Wall Street Journal* article went on to report:

> The risks of doing business with Iran are the same in all currencies," said Mr. [Stuart] Levey. Intelligence officials say Bank Saderat, a large, state-controlled Iranian bank placed on a U.S. Treasury blacklist in October for allegedly funding terrorism, has been able to process dollar transactions through Commerzbank's New York branch in recent months by using the accounts of two other Iranian banks. Commerzbank says it ceased dealing with Saderat after it was put on the U.S. blacklist and has no knowledge of any subsequent transactions. "Commerzbank has no knowledge of Bank Saderat directly or indirectly using the accounts of other Iranian banks to process dollar transactions," the bank said in a statement. Commerzbank, in

> a response to an inquiry from *The Wall Street Journal* about its dealings with Iran, also said "all such [dollar clearing] transactions are currently being phased out" as of Jan. 31. It added that "any clearing conducted by our U.S. operations is in strict compliance" with U.S. government regulations.

1196. Commerzbank's assurances to *The Wall Street Journal,* like its assurances to U.S. Treasury Deputy Secretary Robert Kimmitt, were plainly false.

1197. As noted above, on September 10, 2008, the U.S. designated IRISL, IRISL Europe GmbH, and several IRISL subsidiaries based on evidence that the IRISL network of companies was engaged in WMD proliferation activity and the fact that "IRISL has pursued new strategies which could afford it the potential to evade future detection of military shipments."

1198. The next day, on September 11, 2008, a senior official at OFAC personally forwarded the press release announcing IRISL's SDN designation to the Head of Compliance at Commerzbank in New York.

1199. The press release was then forwarded to Commerzbank employees in Germany with responsibilities related to IRISL. In the email, the relationship manager noted that the U.S. government alleged "that IRISL as Iranian government carrier systematically circumvents the Iranian arms embargo."

1200. Nonetheless, between September 10, 2008, and December 31, 2008 alone, Commerzbank illegally directed close to $40 million on behalf of IRISL subsidiaries and related entities through the United States.

O. DEFENDANT COMMERZBANK AG'S DIRECT FUNDING OF HEZBOLLAH THROUGH ITS CUSTOMER, ORPHANS PROJECT LEBANON e.V.

1201. During this same time period, Commerzbank also maintained account number 7001688, knowing, or with deliberate indifference to the fact, that it was for an open and notorious

Hezbollah fundraising organization in Germany known as Waisenkinderprojekt Libanon e.V. ("the Orphans Project Lebanon e.V.").

1202. Despite prior public German government reports identifying its customer as a Hezbollah fundraising organization, and the fact that on July 24, 2007 the United States designated[76] the Lebanese organization that was primary recipient of funds donated from the account (Hezbollah's Martyrs Foundation), Commerzbank knowingly, or with deliberate indifference to the fact, continued to provide financial services to Waisenkinderprojekt Libanon e.V. and hence continued to transfer funds to Hezbollah.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

CIVIL LIABILITY UNDER 18 U.S.C. § 2333(a) AGAINST ALL DEFENDANTS FOR VIOLATIONS OF 18 U.S.C. § 2339A CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1203. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1204. By knowingly agreeing to provide, and providing, material support to Iran and its agents in an illegal manner, and knowing, or with deliberate indifference to the fact, that some of the objects and aims of the Conspiracy were to be used in preparation for or carrying out multiple acts set forth in 18 U.S.C. § 2339A, each Defendant violated § 2339A's express prohibition against conspiring to provide material support within the meaning of § 2339A, and committed and completed overt acts in furtherance of the Conspiracy.

1205. Each Defendant's conduct in agreeing to provide Iran and its agents with hundreds of millions (or more) of USD in an illegal manner, violated 18 U.S.C. § 2339A's express

[76] *See,* https://www.treasury.gov/press-center/press-releases/Pages/hp503.aspx

prohibition against concealing or disguising the nature, location, source, or ownership of material support or resources, knowing that the material support or resources are to be used in preparation for, or in carrying out, a violation of any of 18 U.S.C. §§ 32, 37, 81, 175, 229, 351, 831, 842(m)-(n), 844(f) or (i), 930 (c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442, 42 U.S.C. § 2284, 49 U.S.C. §§ 46502 or 60123 (b), or any offense listed in 18 U.S.C. § 2332b (g)(5)(B) (except for §§ 2339A and 2339B), as well as conspiring to provide and conceal or disguise the provision of such material support.

1206. Both the Conspiracy itself and the acts of international terrorism that injured the Plaintiffs constitute acts of international terrorism under 18 U.S.C. § 2331, and constitute "engaging in terrorist activity" under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or "engaging in terrorism" under 22 U.S.C. § 2656f.

1207. The Conspiracy between Iran and its agents and the Defendants (including Defendants John Does 1-50), and other non-defendant Co-conspirators resulted in the transfer of: (a) more than two hundred billion dollars through the United States in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies; and (b) hundreds of millions of dollars to Hezbollah, the IRGC and other terrorist organizations (including the Special Groups) actively engaged in murdering and maiming U.S. nationals in Iraq.

1208. The Defendants (including Defendants John Does 1-50) together with other non-defendant Co-conspirators (including Iran) agreed to, and did in fact, purposefully transfer billions of USD through the United States knowing that such funds would be delivered to Iran and Iranian agents, and that the payment order messages facilitating such funds transfers had been deliberately and intentionally structured, designed, and processed in a manner expressly designed to ensure

that such funds would not be detected or monitored by U.S. regulators and law enforcement agencies.

1209. At the time each Defendant knowingly agreed to provide Iran material support in an illegal manner, each Defendant knew that the United States had formally designated Iran as a State Sponsor of Terrorism and knew, or was deliberately indifferent to the fact that, *inter alia*, Iran used the IRGC and Hezbollah as primary mechanisms to cultivate, support and perpetrate terrorism.

1210. Among other things, and as documented in the U.S. State Department's 2013 Country Reports on Terrorism, between 2004 and 2011 the IRGC, in concert with Hezbollah, provided training outside of Iraq, as well as sending advisors to Iraq, to assist, train, supply and guide Special Groups in the construction and use of EFPs and other advanced weaponry, devices that constitute "weapons of mass destruction" as defined in 18 U.S.C. § 2332a, incorporating the definition of "destructive devices" set forth in 18 U.S.C. § 924(4)(A)-(C).

1211. Each Defendant knew or was deliberately indifferent to the fact that Iran, the IRGC, Hezbollah, and the Special Groups engaged or engages in terrorist activity (8 U.S.C. § 1182(a)((3)(B)(iii)-(iv)), terrorism (22 U.S.C § 2656f), and acts of international terrorism (18 U.S.C. § 2331), including facilitating, funding, preparing for, and supporting terrorist activity by the Special Groups.

1212. Through this clandestine stream of U.S. dollars, each Defendant knew, or was deliberately indifferent to the fact that as a result of knowingly agreeing to join the Conspiracy to provide Iran with illegal material support, such conduct foreseeably (and in fact did) facilitate the transfer of hundreds of millions of dollars in payments to the IRGC and Hezbollah through the

international financial system, including payments initiated, processed, altered, modified, falsified, or released by or through the Defendants.

1213. Each Defendant knowingly and purposefully agreed to provide, and to conceal and disguise the provision of, material support and services to Iran in an illegal manner, knowing or deliberately indifferent to the fact that such illegal support and services facilitated Iran's clandestine support for the IRGC and Hezbollah, and that such agreements and resultant overt acts and conduct would (and did) foreseeably facilitate acts of international terrorism, terrorist activities, and terrorism, including homicides, attempted homicides, or conspiracies to commit homicide against U.S. nationals by the IRGC, Hezbollah and the Special Groups (including KH, JAM and AAH), as well as attacks conducted by weapons of mass destruction, such as EFPs, and bombings, attempted bombings, or conspiracies to bomb places of public use, state or government facilities, public transportation systems, or infrastructure facilities by the IRGC, Hezbollah, and the Special Groups.

1214. The material support that Defendants knowingly agreed to illegally provide to Iran and its agents, including concealing or disguising the nature, location, source, or ownership of material support or resources, provided foreseeable, substantial assistance to the IRGC, Hezbollah and the Special Groups, thereby preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries.

1215. The material support that Defendants knowingly agreed to illegally provide, and conceal and disguise the provision of, to Iran and its agents included facilitating tens of millions of dollars in illicit transactions on behalf of MODAFL, the IRGC, Mahan Air and other instrumentalities of Iranian state-sponsored terror to enable numerous violations of the U.S. trade

embargo against Iran, concealing Iran's efforts to evade U.S. sanctions and enabling Iran's acquisition from the United States of goods and technologies prohibited by U.S. law to be sold or transferred to Iran, including components of IEDs deployed against Coalition Forces in Iraq.

1216. Each Defendant also: knew of the existence of other conspirators including some or all of the Defendants; was aware that the other conspirators (including Defendants and Iranian Bank Co-conspirators) engaged in the same or similar conduct, and that the other conspirators shared the objective of providing material support to Iran and its agents in an illegal manner for the explicit purpose of enabling Iran to avoid U.S. sanctions and regulations enacted specifically to prevent Iran's ability to finance, support, prepare for, plan, or carry out acts of international terrorism, including the types of acts that injured the Plaintiffs.

1217. Each Defendant knew that the U.S. sanctions and regulations it helped Iran and its agents violate were enacted specifically to prevent Iran's ability to finance, support, prepare for, plan, or carry out acts of international terrorism, including the types of acts that injured the Plaintiffs.

1218. Each Defendant also knew or was deliberately indifferent to the fact that one of the specific aims and objectives of the Conspiracy was keeping U.S. depository institutions, law enforcement and counter-terrorism agencies blind to Iran's movement of U.S. dollars through the international financial system, and thus also knew or was deliberately indifferent to the fact that the overt acts they performed in furtherance of the Conspiracy facilitated that specific objective.

1219. Having entered into an agreement to provide Iran material support in an illegal manner, in direct contravention of U.S. laws and regulations enacted expressly to mitigate Iran's sponsorship of terrorism and terrorist organizations (including Weapons of Mass Destruction proliferation activities in furtherance of such sponsorship) each Defendant also knew or was

deliberately indifferent to the fact, that the Conspiracy's aims would foreseeably result in Iran transferring millions of dollars in order to engage in terrorist activities (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331).

1220. The Defendants' overt acts and agreement to purposefully transfer billions of dollars through the United States to Iran in a manner expressly designed to ensure that the funds could be transferred by and to Iran without being monitored by U.S. regulators and law enforcement agencies, involved acts that were dangerous to human life, by their nature, and as further evidenced by their consequences.

1221. The Defendants' acts either occurred primarily outside the territorial jurisdiction of the United States or transcended national boundaries in terms of the means by which they were accomplished.

1222. Each Defendant's agreement to enter into the Conspiracy and purposeful transfer of billions of dollars through the United States in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies foreseeably resulted in material support being delivered in order to carry out or prepare for violations of, *inter alia*, 18 U.S.C. §§ 2332(a)-(c), 2332a, and § 2332f by the IRGC, Hezbollah and the Special Groups, and were thus themselves acts of international terrorism because they objectively appeared to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating the IRGC, Hezbollah and the Special Groups' abilities to prepare for, support, fund, train, initiate, and/or carry out mass destruction, murder, and kidnapping.

1223. Each Defendant's conduct was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries, and foreseeably, substantially enhanced the IRGC, Hezbollah and the Special Groups' ability to engage in terrorist activity (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and/or commit acts of international terrorism (18 U.S.C. § 2331) (including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f and 2339A). Each Defendant's conduct was thus also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1224. Furthermore, each Plaintiff's injuries were caused by unlawful overt acts performed by at least one of the parties to the Conspiracy, which act was a foreseeable consequence of the Conspiracy.

1225. Each Plaintiff's injuries constitutes a harm falling within the foreseeable risk contemplated by each Defendant's violations, including each Defendant's knowing agreement to enter into the Conspiracy, each Defendant's performance of overt acts in furtherance of the Conspiracy, and each Defendant's knowledge or deliberate indifference to the full scope, objectives, and results of the Conspiracy. Injuries resulting from terrorist attacks (including attacks launched by the IRGC, Hezbollah and the Special Groups) that were planned, supported by, funded, or assisted by Iran are precisely the risks contemplated by Executive Orders, statutes and regulations (including, without limitation, designations under Executive Orders specifically concerning the IRGC, Defendant Bank Saderat Plc, and IRISL) enacted specifically to ensure that Iran had restricted access to USD and financial services under conditions of maximum transparency, that such dollars were used only for legitimate agencies, operations, and programs and not by or for the benefit of SDNs, and not for Iran's efforts to acquire, develop, and distribute Weapons of Mass Destruction (including weapons such as EFPs directed at Coalition Forces), and

to ensure that any funds Iran did receive that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies.

1226. Through its conduct as described above, by knowingly entering into the Conspiracy and violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged above, each Defendant committed acts of international terrorism and is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

SECOND CLAIM FOR RELIEF

CIVIL LIABILITY UNDER 18 U.S.C. § 2333(a) AGAINST ALL DEFENDANTS FOR VIOLATIONS OF 18 U.S.C. § 2339B CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1227. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1228. In knowingly agreeing to provide, and providing, material support to Iran and its agents in an illegal manner, and knowing, or deliberately indifferent to the fact, that the objects and aims of the Conspiracy included providing material support to Foreign Terrorist Organizations (FTOs), including Hezbollah and Kata'ib Hezbollah, each Defendant violated § 2339B's express prohibition against conspiring to provide material support within the meaning of § 2339B, and committed and completed overt acts in furtherance of the Conspiracy

1229. The Defendants herein (including Defendants John Does 1-50) and Iran and its agents agreed to, and did in fact, purposefully transfer hundreds of billions of dollars through the United States in a manner expressly designed to circumvent monitoring by U.S. regulators and law enforcement agencies and evade U.S. sanctions; minimize the transparency of their financial activities; and knowingly, or with deliberate indifference, facilitated the transfer of tens of millions of dollars in payments to Hezbollah through the international financial system. In doing so, the

Defendants were willing to, and did, commit numerous felonies under U.S. law to assist Iran in concealing its financial activities and violated 18 U.S.C. § 2339B by knowingly, or with deliberate indifference, entering the Conspiracy, the objects and aims of which included providing material support to FTOs that were responsible for Plaintiffs' injuries.

1230. At the time each Defendant knowingly agreed to assist Iran and its agents in an illegal manner, each Defendants knew that Iran had, since 1984, been officially designated by the United States as a State Sponsor of Terrorism, subject to various U.S. sanctions, and knew that such designation was based in part on Iran's sponsorship and patronage of Hezbollah and other FTOs, and that Iran used Hezbollah as a primary mechanism to enable it to cultivate and support terrorism.

1231. Each Defendant knew, or was deliberately indifferent to the fact that, Hezbollah was designated an FTO at all times relevant to this action. Each Defendant also knew that Hezbollah engaged in terrorist activities (8 U.S.C. § 1183(a)(3)(B)(iii)-(iv)), terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331).

1232. Each Defendant knew or was deliberately indifferent to the fact that its agreement to join the Conspiracy to launder billions of dollars knowing or deliberately indifferent to the fact that its objects and aims included providing material support to FTOs in an illegal manner, and that the overt acts it completed in connection with the Conspiracy unlawfully evaded U.S. sanctions and regulations directed at preventing Iran from carrying out, supporting, funding, planning for, preparing, conspiring with, or facilitating acts of international terrorism by FTOs, including acts planned, attempted, and perpetrated by Iran's proxy, agent, and strategic partner, Hezbollah.

1233. Both the Conspiracy itself and the acts of international terrorism that injured the Plaintiffs constitute acts of international terrorism under 18 U.S.C. § 2331, and constitute "engaging in terrorist activity" under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or "engaging in terrorism" under 22 U.S.C. § 2656f.

1234. Each Defendant also: knew of the existence of other Co-conspirators including some or all of the Defendants; was aware that the other Co-conspirators (including the other Defendants and Iranian Bank Co-conspirators) engaged in the same or similar conduct, and that the other Co-conspirators agreed to join a the Conspiracy knowing or deliberately indifferent to the fact that its objects and aims included providing material support to FTOs in an illegal manner for the explicit purpose of enabling Iran to avoid U.S. sanctions and regulations enacted specifically to prevent Iran's ability to finance, support, prepare for, plan, or carry out acts by FTOs including Iran's proxy, agent, and strategic partner, Hezbollah.

1235. Each Defendant also knew or was deliberately indifferent to the fact that one of the specific aims and objectives of the Conspiracy was to keep U.S. depository institutions, law enforcement and counter-terrorism agencies blind to Iran's movement of U.S. dollars through the international financial system, and thus also knew or was deliberately indifferent to the fact that the overt acts it performed in furtherance of the Conspiracy facilitated that specific objective.

1236. Having entered into an agreement to contravene U.S. laws and regulations enacted expressly to mitigate Iran's sponsorship of terrorism and terrorist organizations (including Weapons of Mass Destruction proliferation activities in furtherance of such sponsorship) by laundering funds in order to blind U.S. regulators, law enforcement and counter-terrorism authorities, each Defendant also knew or was deliberately indifferent to the Conspiracy's

corresponding objectives and aims, including transferring millions of dollars to Iran's proxy, Hezbollah, an FTO.

1237. The material support that each Defendant, through the Conspiracy, knowingly, or with deliberate indifference, provided to Hezbollah, constituted substantial assistance to Hezbollah, thereby facilitating acts of terrorism in violation of §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f, and that have caused injuries to Plaintiffs.

1238. The Defendants' overt acts in entering into the Conspiracy and knowingly agreeing to contravene U.S. laws designed to prevent Iran – a known and designated State Sponsor of Terrorism – from providing material support to FTOs, and the resultant, purposeful transfer of billions of USD through the United States in a manner expressly designed to ensure that the funds could be transferred without being monitored by U.S. regulators and law enforcement agencies, involved acts that were dangerous to human life, by their nature, and as further evidenced by their consequences.

1239. The Defendants' acts either occurred primarily outside the territorial jurisdiction of the United States or transcended national boundaries in terms of the means by which they were accomplished.

1240. Each Defendant's agreement to enter into the Conspiracy and purposeful transfer (collectively) of billions of dollars through the United States in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies foreseeably resulted in material support being provided to FTOs, and were thus themselves acts of international terrorism because they objectively appeared to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion (in part to cause them to withdraw

Coalition Forces from Iraq), and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Hezbollah's role in killing, kidnapping and injuring hundreds of American nationals in Iraq (including by mass destruction).

1241. Each Defendant's conduct was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries, and foreseeably, substantially accelerated and multiplied Hezbollah's ability to engage in terrorist activity (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism under the definition set forth in 18 U.S.C. § 2331. Each Defendant's conduct was thus also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1242. Furthermore, each Plaintiff's injuries were caused by unlawful overt acts performed by at least one of the parties to the Conspiracy, which act was a foreseeable consequence of the Conspiracy.

1243. Each Plaintiff's injuries constitutes a harm falling within the risk contemplated by each Defendant's violations, including each Defendant's knowing agreement to enter into the Conspiracy, the overt acts each Defendant performed in furtherance of the Conspiracy, and each Defendant's knowledge of, or deliberate indifference to, the fact that a specific, foreseeable aim and purpose of the Conspiracy was to provide material support to Hezbollah and other FTOs. Injuries resulting from terrorist attacks planned, designed, assisted, funded, initiated, and/or overseen by Hezbollah are precisely the risks contemplated by statutes, regulations and Executive Orders designed to ensure that Hezbollah's sponsor, principal, and strategic partner – Iran – had restricted access to U.S. dollars and financial services, and that any funds it did receive that touched U.S. depository institutions were transparent and could be blocked if warranted.

1244. Through its conduct as described above, by knowingly entering into the Conspiracy and violating 18 U.S.C. § 2339B in the manner and with the state of mind alleged above, each Defendant committed acts of international terrorism and is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

THIRD CLAIM FOR RELIEF

CIVIL LIABILITY AGAINST HSBC BANK USA, N.A. UNDER 18 U.S.C. § 2333(a) FOR VIOLATIONS OF 18 U.S.C. § 2332d CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1245. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1246. Defendant HSBC-US is a juridical person organized under the laws of the United States pursuant to 18 U.S.C. § 2332d(b)(2)(C) and is also a person within the United States pursuant to 18 U.S.C. § 2332d(b)(2)(D).

1247. As alleged above, at all relevant times HSBC-US knew that Iran was a country designated by the United States under section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. 2405) as a country supporting international terrorism, yet HSBC-US nevertheless engaged in thousands of financial transactions with Iran in violation of 18 U.S.C. § 2332d.

1248. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that Hezbollah had been designated an FTO.

1249. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that the IRGC-QF had been designated an SDGT.

1250. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that Bank Saderat (including Defendant Bank Saderat Plc) had been designated an SDGT.

1251. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that the IRGC had been designated an SDN.

1252. Defendant HSBC-US also knew or was deliberately indifferent to the fact that Bank Melli (including Melli Bank Plc), Bank Saderat (including Defendant Bank Saderat Plc), Bank Mellat, and Bank Sepah had been designated SDNs before November 2008, and, as such, were excluded from accessing the U-Turn exemption in the Iranian Transaction Regulations.

1253. Defendant HSBC-US also knew or was deliberately indifferent to the fact that the IRISL and multiple IRISL entities had been designated SDNs.

1254. As alleged above, HSBC-US knowingly conducted illegal financial transactions on behalf of Iran through Bank Melli and other Iranian counter-parties that did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department – regulations passed for the specific purposes of mitigating the risk that funds transfers to Iran could be used to: engage in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, or acts of international terrorism under 18 U.S.C. § 2331.

1255. In fact, the transactions at issue (including at least the $183 million HSBC-US facilitated on behalf of sanctioned entities in Iran that were identified in HSBC-US's December 11, 2012 Deferred Prosecution Agreement with DOJ) explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203.

1256. Defendant HSBC-US knew that Defendants HSBC-Europe and HSBC-Middle East were deliberately altering and omitting information in funds transfer payment order messages being processed through HSBC-US, thereby evading U.S. laws and regulations whose express purpose was (and is) to ensure that only a very limited class of payments could be facilitated to Iran, and that payment order messages for such funds transfers required transparency in order to ensure that the transfers qualified for the limited exceptions and exemptions, and did not result in U.S. depository institutions processing transactions for the benefit of SDNs.

1257. As alleged in detail above, throughout the relevant time period, HSBC-US knew that other HSBC Defendants such as HSBC-London and HSBC-Middle East were providing material support to Iran in a manner violating U.S. laws and regulations, and HSBC-US also knew its own systems and networks were being used to facilitate the HSBC Defendants' illegal conduct.

1258. Defendant HSBC-US also thus knew or was deliberately indifferent to the fact that Iran, the IRGC, IRISL, Hezbollah, and Defendant Bank Saderat Plc all engaged in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, and acts of international terrorism under 18 U.S.C. § 2331 (including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f), and that Iran provided massive support and sponsorship for violations of all these statutes, while also providing support for other acts of international terrorism, such as those planned, attempted, and perpetrated by the Special Groups.

1259. Knowing that Defendants HSBC-London and HSBC-Middle East were moving billions of sanctions-evading Iranian USD through HSBC-US's offices with the specific intent of defeating HSBC-US's OFAC filters and violating HSBC-US reporting requirements, it was reasonably foreseeable that HSBC-US's conduct would aid Iran and Iran's agents, proxies, and strategic partners (including Hezbollah, the IRGC, and Special Groups) to engage in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, and acts of international terrorism under 18 U.S.C. § 2331.

1260. Because Defendant HSBC-US is a financial institution operating in the United States, at all times relevant to the Amended Complaint, it is deemed by law to be aware of all designations made to the SDN list, including without limitation designations for Iran, Hezbollah, the IRGC, the IRGC-QF, Bank Saderat (including Defendant Bank Saderat Plc), Bank Melli, Bank Mellat, Bank Sepah, IRISL (and multiple IRISL entities).

1261. Defendant HSBC-US thus also knew or was deliberately indifferent to the fact that Bank Melli (including Melli Bank Plc), Bank Saderat (including Defendant Bank Saderat Plc) Bank Mellat, and Bank Sepah had been designated SDNs before November 2008, and, as such, were excluded from accessing the U-Turn exemption in the Iranian Transaction Regulations.

1262. Defendant HSBC-US's conduct foreseeably and substantially enhanced Hezbollah's, the IRGC's and the Special Groups' and other Iranian-sponsored terrorists' ability to engage in terrorist activity, including preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus HSBC-US's conduct was also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1263. Defendant HSBC-US's knowing or deliberately indifferent provision of illegal financial services to Iran, enabled Iran to move billions of U.S. dollars through the United States without those funds being monitored by U.S. regulators and law enforcement agencies and therefore involved acts that were dangerous to human life, by their nature and as evidenced by their consequences.

1264. Defendant HSBC-US's acts transcended national boundaries in terms of the means by which they were accomplished.

1265. Defendant HSBC-US's conduct itself constitutes an act of international terrorism because it either was, or objectively appears to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Iran's ability to prepare for and/or carry out mass destruction and murder.

1266. Furthermore, each Plaintiff's injuries constitute a harm falling within the risk contemplated by Defendant HSBC-US's violations, including its knowing agreement to provide illegal services to Iran. Injuries resulting from terrorist attacks (including attacks launched by Hezbollah through its proxies) that were planned, supported by, funded, or assisted by the IRGC and/or Hezbollah are precisely the risks contemplated by Executive Orders, statutes and regulations designed to ensure that Iran had restricted access to U.S. dollars and financial services, and that any funds it did receive that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies, and that the transactions were not for the benefit of SDNs.

1267. Through its conduct as described above, by violating § 2332d in the manner and with the state of mind alleged above, HSBC-US committed acts of international terrorism, and is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

FOURTH CLAIM FOR RELIEF

CIVIL LIABILITY UNDER 18 U.S.C. § 2333(a) AGAINST STANDARD CHARTERED BANK, ROYAL BANK OF SCOTLAND N.V. AND COMMERZBANK FOR VIOLATIONS OF 18 USC § 2332d CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1268. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1269. Defendants SCB, ABN Amro (RBS N.V.), and Commerzbank each utilized their respective New York branches in connection with their agreement to provide Iran material support in an illegal manner in order to effectuate and facilitate the Conspiracy, and each of those respective New York branches is a "person in the United States" within the scope of 18 U.S.C. § 2332d(b)(2)(D).

1270. As set forth above, each of the above-referenced Defendants knew or was deliberately indifferent to the fact that Iran was designated under section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. 2405) as a country supporting international terrorism and nonetheless knowingly engaged in thousands of illegal financial transactions with the government of Iran through their U.S. operations.

1271. The New York branch of each of the above-referenced Defendants also knew, or was deliberately indifferent to the fact, that Hezbollah had been designated an FTO, that the IRGC-QF and Bank Saderat (including Defendant Bank Saderat Plc) had each been designated an SDGT, and that multiple other Iranian actors and agents (including the IRGC, Bank Melli, Bank Mellat, Bank Sepah, IRISL (and multiple IRISL entities)) had been designated SDNs.

1272. The New York branches of the above-referenced Defendants also knew or were deliberately indifferent to the fact that Bank Melli (including Melli Bank Plc), Bank Saderat (including Defendant Bank Saderat Plc), Bank Mellat, and Bank Sepah had been designated SDNs before November 2008, and, as such, were excluded from accessing the U-Turn exemption in the Iranian Transaction Regulations.

1273. As set forth above, the illegal transactions knowingly facilitated through New York by the respective New York branches of the above-referenced Defendants thus did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department for U-Turn exemption transactions, and therefore violated the criminal provisions of 18 U.S.C § 2332d(a).

1274. In fact, the transactions at issue explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203.

1275. Each of the above-referenced Defendants' New York branch's acts transcended national boundaries in terms of the means by which they were accomplished.

1276. Each of the above-referenced Defendants' New York branch's conduct foreseeably and substantially enhanced Hezbollah's, the IRGC's and Special Groups' and other Iranian sponsored terrorists' ability to engage in terrorist activity, including preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus each of the above Defendants' New York branch's conduct was also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1277. Each of the above-referenced Defendant's New York branch knowingly, or with deliberate indifference, provided financial services to Iran in the United States, knowing that its conduct enabled Iran to move millions (or in some cases, billions) of USD through the United States without those funds being monitored by U.S. regulators and law enforcement agencies. That conduct involved acts that were dangerous to human life, by their nature and as evidenced by their consequences.

1278. Each of the above-referenced Defendant's conduct itself constitutes an act of international terrorism because it either was, or objectively appears to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Iran's ability to prepare for and/or carry out mass destruction and murder.

1279. Furthermore, each Plaintiff's injuries constitute a harm falling within the risk contemplated by each of the above-referenced Defendants' New York branch's unlawful conduct, including their knowing agreement to provide illegal services to Iran. Injuries resulting from terrorist attacks committed, planned, or authorized by Hezbollah and the IRGC and carried out by their proxies, the Special Groups are precisely the risks contemplated by Executive Orders, statutes

and regulations designed to ensure that Iran had restricted access to U.S. dollars and financial services, and that any funds it did receive that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies.

1280. Each of the above-referenced Defendants' criminal violations of the provisions of 18 U.S.C. § 2332d(a) was a sufficient cause of Plaintiffs' injuries, and, for the reasons alleged in Plaintiffs' Third Claim for Relief against Defendant HSBC-US, constitutes an act of international terrorism rendering each of the above Defendants civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

FIFTH CLAIM FOR RELIEF

CIVIL LIABILITY AGAINST COMMERZBANK AG UNDER 18 U.S.C. § 2333(a) FOR VIOLATIONS OF 18 U.S.C. § 2339A CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1281. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1282. Defendant Commerzbank provided material support to the IRGC through Commerzbank's acts on behalf of IRISL, and Commerzbank violated § 2339A in concealing and disguising the nature, location, source, and ownership of material support it provided to IRISL, knowing or deliberately indifferent to the fact, that IRISL and the IRGC would use that support in preparation for, or in carrying out acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f .

1283. Defendant Commerzbank knew or was deliberately indifferent that to the fact that the IRISL had been designated an SDN for Weapons of Mass Destruction-related activities that included arms shipments, including shipments destined for Hezbollah and other terrorists.

1284. Defendant Commerzbank's conduct was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries, and substantially accelerated and multiplied the IRGC's ability to engage in terrorist activity (8 U.S.C § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and/or commit acts of international terrorism as that terms is defined in 18 U.S.C. § 2331.

1285. The material support that Commerzbank knowingly and illegally provided to the IRISL provided foreseeable, substantial assistance to the IRGC, Hezbollah and the Special Groups, thereby preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus Commerzbank's conduct was also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1286. Commerzbank's illegal conduct transcended national boundaries in terms of the means by which it was accomplished.

1287. Commerzbank's knowing or deliberately indifferent provision of illegal financial services to the IRGC and IRISL involved acts that were dangerous to human life, by their nature and as evidenced by their consequences.

1288. Commerzbank's conduct itself constitutes an act of international terrorism because it either was, or objectively appears to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Iran's ability to prepare for and/or carry out mass destruction and murder.

1289. Furthermore, each Plaintiff's injuries constitute a harm falling within the risk

contemplated by Commerzbank's material support to the IRGC and IRISL. Injuries resulting from terrorist attacks perpetrated, planned, supported by, funded, or assisted by Iran and Hezbollah are precisely the risks contemplated by statutes and regulations designed to ensure that the IRGC, IRISL and Iran had restricted access to USD and financial services, and that any funds they did receive that touched U.S. depository institutions were transparent and could be blocked if warranted, and did not benefit an SDN.

1290. Through its conduct as described above, by knowingly or with deliberate indifference, providing material support to Iran, the IRGC, and IRISL, and thereby violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged above, Commerzbank is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

SIXTH CLAIM FOR RELIEF

CIVIL LIABILITY AGAINST COMMERZBANK AG UNDER 18 U.S.C. § 2333(a) FOR VIOLATIONS OF 18 U.S.C. § 2339B CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1291. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1292. Defendant Commerzbank violated § 2339B by providing material support to Hezbollah through Commerzbank's acts on behalf of its customer Waisenkinderprojekt Libanon e.V. (Orphans Project Lebanon e.V.).

1293. Commerzbank knew, or was deliberately indifferent to the fact, that Orphans Project Lebanon e.V. was transferring funds through Commerzbank to FTO Hezbollah and that Hezbollah would use that support in preparation for, or in carrying out, acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f.

1294. Defendant Commerzbank's conduct was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries, and substantially accelerated and multiplied Hezbollah's ability to engage in terrorist activity (8 U.S.C § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism as that terms is defined in 18 U.S.C. § 2331.

1295. The material support that Commerzbank knowingly and illegally provided to the Orphans Project Lebanon e.V. and hence to Hezbollah, provided foreseeable, substantial assistance to the Hezbollah and the Special Groups, thereby preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus Commerzbank's conduct was also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1296. Commerzbank's illegal conduct transcended national boundaries in terms of the means by which it was accomplished.

1297. Commerzbank's knowing or deliberately indifferent provision of illegal financial services to Hezbollah involved acts that were dangerous to human life, by their nature and as evidenced by their consequences.

1298. Commerzbank's conduct itself constitutes an act of international terrorism because it either was, or objectively appears to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Iran's ability to prepare for and/or carry out mass destruction and murder.

1299. Furthermore, each Plaintiff's injuries constitute a harm falling within the risk

contemplated by Commerzbank's material support to Hezbollah.

1300. Through its conduct as described above, by knowingly or with deliberate indifference, providing material support to Hezbollah, and thereby violating 18 U.S.C. § 2339B in the manner and with the state of mind alleged above, Commerzbank is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

SEVENTH CLAIM FOR RELIEF

CIVIL LIABILITY AGAINST STANDARD CHARTERED BANK UNDER 18 U.S.C. § 2333(a) FOR VIOLATIONS OF 18 U.S.C. § 2339A CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

1301. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1302. Defendant Standard Chartered Bank provided material support to the IRGC and its Qods Force through its acts on behalf of the IRGC's agent NIOC, Mahan Air, MODAFL and other entities identified *supra* in violation of § 2339A by concealing and disguising the nature, location, source, and ownership of material support it provided to the IRGC's agent NIOC, Mahan Air, MODAFL and other entities identified *supra*, knowing or deliberately indifferent to the fact that the IRGC and its Qods Force would use that support in preparation for, or in carrying out, acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f .

1303. Defendant Standard Chartered Bank knew or was deliberately indifferent to the fact that the IRGC's agent NIOC, Mahan Air, MODAFL and other entities identified *supra* were utilizing Letters of Credit facilitated by Standard Chartered Bank to evade U.S. sanctions and acquire materials used, *inter alia*, to effectuate arms shipments, transport weapons, personnel and technology to the IRGC-QF and Hezbollah.

1304. Mahan Air did, in fact, transport weapons, personnel and technology into Iraq on behalf of the IRGC-QF and Hezbollah and did, in fact, transport modules used to control and activate IEDs and EFPs deployed against Coalition Forces in Iraq.

1305. Iran could not have successfully evaded U.S. sanctions and obtained raw materials and manufacturing equipment prohibited by the International Traffic in Arms Regulations ("ITARs"), Export Administration Regulations ("EARs"), and Iran Trade Regulations ("ITRs") simply by establishing front companies in foreign jurisdictions like Malaysia, Singapore or Dubai because those front companies could not have negotiated international payments without being able to provide U.S. and other suppliers with conventional letters of credit drawn on Western banks with established correspondent accounts with U.S. clearing banks.

1306. Nor could the front companies that participated in Iran's clandestine supply chain have succeeded in their efforts had they been forced to rely solely on financing by Iranian banks because those banks could not have provided financing directly since they could not maintain correspondent accounts with U.S. clearing banks and most of them were blacklisted at one point in time or another and frozen out of the US dollar-clearing system.

1307. For example, no legitimate U.S. manufacturer would have agreed to transport materials subject to the ITARs, EARs or ITRs to an unknown company in Singapore or Dubai based on a letter of credit issued by Bank Saderat or Bank Melli.

1308. The linchpin of Iran's illegal and clandestine supply chain was the cooperation of Standard Chartered Bank and the other Western Bank Defendants that concealed both the role of Iranian banks in providing the credit necessary to finance the transactions and the identities of the Iranian military and IRGC sub-agencies that were actually purchasing the raw materials and manufacturing equipment (invariably being transported to Iran by IRISL, Mahan Air or Iran Air).

1309. Defendant Standard Chartered Bank knew, or was deliberately indifferent to the fact, that the IRGC's agent NIOC, Mahan Air, MODAFL and other entities identified *supra* were utilizing Letters of Credit facilitated by Standard Chartered Bank to evade U.S. sanctions and acquire materials used, *inter alia*, to effectuate arms shipments, transport weapons, personnel and technology to the IRGC-QF and Hezbollah.

1310. Mahan Air did, in fact, transport weapons, personnel and technology into Iraq on behalf of the IRGC-QF and Hezbollah and did, in fact, transport modules used to control and activate IEDs and EFPs deployed against Coalition Forces in Iraq.

1311. With the necessary assistance of Standard Chartered Bank and the other Western Bank Defendants, MODAFL did in fact acquire spare parts for various military aircraft.

1312. With the necessary assistance of Standard Chartered Bank and the other Western Bank Defendants, Iranian front companies did purchase hydraulic press components of the kind used to manufacture EFPs and did purchase steel and copper and other materials necessary for the manufacturing of EFPs and other weapons deployed against Coalition Forces in Iraq.

1313. This substantial assistance to Iran's terror apparatus (including the IRGC and MODAFL), knowingly provided by Defendant Standard Chartered Bank, made it possible for Iran to procure the radio frequency modules, metals, and hydraulic presses used to manufacture the copper plates and steel cylinders necessary to manufacture the EFPs and other Iranian weapons used in the attack injuring the Plaintiffs, as well Iran's transport of weapons, supplies, and IRGC and Hezbollah operatives (who conducted, supervised, and trained the perpetrators of those attacks).

1314. Defendant Standard Chartered Bank's conduct was a substantial cause in fact and a significant factor in the chain of events leading to the Plaintiffs' injuries, and substantially

accelerated and multiplied the IRGC's ability to engage in terrorist activity (8 U.S.C § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and commit acts of international terrorism as that terms is defined in 18 U.S.C. § 2331.

1315. The material support that Standard Chartered Bank knowingly and illegally provided to the IRGC's agent NIOC, Mahan Air, MODAFL and other entities identified *supra* provided foreseeable, substantial assistance to the IRGC, Hezbollah and the Special Groups, thereby preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus Standard Chartered Bank's conduct was also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

1316. Standard Chartered Bank's illegal conduct transcended national boundaries in terms of the means by which it was accomplished.

1317. Standard Chartered Bank's knowing or deliberately indifferent provision of illegal financial services to the IRGC, the IRGC's agent, NIOC, Mahan Air, MODAFL and other entities identified *supra*, involved acts that were dangerous to human life, by their nature and as evidenced by their consequences.

1318. Standard Chartered Bank's conduct itself constitutes an act of international terrorism because it either was, or objectively appears to have been intended to: (a) intimidate or coerce the civilian population of the United States and other nations, (b) influence the policy of the governments of the United States and other nations by intimidation or coercion, and/or (c) affect the conduct of the governments of the United States and other nations by facilitating Iran's ability to prepare for and/or carry out mass destruction and murder.

1319. Furthermore, each Plaintiff's injuries constitute a harm falling within the risk contemplated by Standard Chartered Bank's material support to the IRGC, the IRGC's agent, NIOC, Mahan Air, MODAFL and other entities identified *supra*. Injuries resulting from terrorist attacks perpetrated, planned, supported by, funded, or assisted by Iran and Hezbollah are precisely the risks contemplated by statutes and regulations designed to ensure that Iran had restricted access to U.S. dollars and financial services, and that any funds they did receive that touched U.S. depository institutions were transparent and could be blocked if warranted, and did not benefit an SDN.

1320. Through its conduct as described above, by knowingly or with deliberate indifference, providing material support to Iran, the IRGC, the IRGC's agent, NIOC, Mahan Air, MODAFL and other entities identified *supra*, and thereby violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged above, Standard Chartered Bank is civilly liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

EIGHTH CLAIM FOR RELIEF

CIVIL LIABILITY FOR CONSPIRACY IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (JASTA)

1321. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1322. The attack alleged herein was an act of international terrorism as defined by 18 U.S.C. § 2331(1).

1323. Hezbollah was designated as a Foreign Terrorist Organization on October 8, 1997 and was so designated as of the date the attack alleged herein was committed.

1324. The IRGC was designated as a Foreign Terrorist Organization on April 15, 2019, in part for its role in the attack at issue.

1325. The IRGC and Hezbollah provided the RPG-29 used in the attack against Coalition Forces that injured the Plaintiffs.

1326. The IRGC and Hezbollah funded, trained, equipped, guided, directed and controlled the cells and individuals who injured the Plaintiffs in concert with, and at the direction of, the IRGC and Hezbollah.

1327. The IRGC and Hezbollah together with their Iraqi agents and proxies, including the Special Groups, jointly committed, planned and authorized the attack.

1328. Defendants entered into the Conspiracy to launder billions of dollars clandestinely on behalf of Iranian banks, designated Iranian entities and NIOC, and to conceal illicit Iranian transactions through the United States from U.S. regulators, law enforcement and counter-terrorist financing authorities.

1329. Defendants entered into the Conspiracy, which included the IRGC (FTO) and Hezbollah (FTO) and their agents and proxies, who were the persons (within the meaning of 18 U.S.C. § 2333(d)(1) and 1 U.S.C. §1) that committed the act of international terrorism set forth herein.

1330. The reasonable foreseeable consequences, and foreseeable risk, of entering into the Conspiracy to launder billions of dollars on behalf of a State Sponsor of Terrorism and designated Iranian entities clandestinely through the United States (in order to conceal these activities from U.S. regulators, law enforcement and counter-terrorist financing authorities) included the clandestine funding of the IRGC and Hezbollah, and preparation for and carrying out of numerous terrorist attacks committed by the IRGC, Hezbollah, and their proxies against U.S. nationals in Iraq.

1331. Each Defendant provided its Iranian counterparties with unusual and unlawful

banking services under unusual circumstances by working closely and interactively with them to maintain the scheme of disguise and concealment, including exchanging secret communications in order to develop and constantly refine unusual and unlawful methods for circumventing U.S. counter-terrorist financing controls.

1332. Each Defendant was aware of the role of other, similar banks (i.e., the other Defendants) in providing similar services for Iran, the IRGC, Hezbollah, and their agents, as part of the Conspiracy. In some cases, Defendants communicated with each other in furtherance of the Conspiracy.

1333. Each Defendant was aware of the role of Iranian governmental and commercial entities in the Conspiracy that sought to evade U.S. sanctions publicly intended to prevent Iranian terror financing.

1334. Plaintiffs' injuries were proximately caused by the IRGC's and Hezbollah's acts of international terrorism.

NINTH CLAIM FOR RELIEF

CIVIL LIABILITY FOR AIDING AND ABETTING IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (JASTA)

1335. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1336. The attack alleged herein was an act of international terrorism as defined by 18 U.S.C. § 2331(1).

1337. Hezbollah was designated as a Foreign Terrorist Organization on October 8, 1997 and was so designated as of the date the attack alleged herein was committed.

1338. The IRGC was designated as a Foreign Terrorist Organization on April 15, 2019, in part for its role in the attack at issue.

1339. The IRGC and Hezbollah together with their Iraqi agents and proxies, including the Special Groups, committed, planned and authorized the attack alleged herein.

1340. The IRGC and Hezbollah provided the RPG-29 used in the attack against Coalition Forces that injured the Plaintiffs.

1341. The IRGC and Hezbollah funded, trained, equipped, guided, directed and controlled the cells and individuals who injured the Plaintiffs in concert with, and at the direction of, the IRGC and Hezbollah.

1342. The IRGC and Hezbollah together with their Iraqi agents and proxies, including the Special Groups, jointly committed, planned and authorized the attack.

1343. Defendants aided and abetted (within the meaning of 18 U.S.C. § 2333(d)(2)), the IRGC (FTO) and Hezbollah (FTO) (and their agents and proxies acting in concert with them and at their direction), who were the persons (within the meaning of 18 U.S.C. § 2333(d)(1) and 1 U.S.C. §1) that committed the act of international terrorism set forth herein.

1344. Each Defendant knowingly provided substantial assistance, directly or indirectly, to the IRGC and its agents (including NIOC, MODAFL, and Mahan Air) and Hezbollah.

1345. Each Defendant was generally aware of its role in the overall illegal and tortious activity of laundering billions of dollars clandestinely on behalf of a State Sponsor of Terrorism, its banks, designated Iranian entities and agents and NIOC (an IRGC agent), to conceal illicit Iranian transactions through the United States from U.S. regulators, law enforcement and counter-terrorist financing authorities.

1346. Each Defendant was generally aware that its acts provided these entities, directly or indirectly, concealed access to the U.S. financial system that enabled Iran to facilitate its support and preparation for, and carrying out of, act of international terrorism.

1347. The nature of the act assisted, a long-running money laundering scheme to launder billions of dollars clandestinely on behalf of Iran, the IRGC, Hezbollah, and their agents, heavily depended on the active and sustained cooperation of Defendants, which were among the largest dollar-clearing banks in the world.

1348. Each Defendant had a continuing and long-term banking relationship with its Iranian counterparties necessary to the assistance they provided—blinding American counter-terrorist-financing authorities to Iran's access to the financial system for the purpose of facilitating material support for terrorism. Each Defendant provided its Iranian counterparties unusual and unlawful banking services under unusual circumstances by working closely and interactively with them to maintain the scheme of disguise and concealment, including exchanging secret communications in order to develop and constantly refine unusual and unlawful methods for circumventing U.S. counter-terrorist financing controls.

1349. Each Defendant knew, or knew of the substantial certainty, that some of the funds it disguised and concealed would be used by Iran, the IRGC, Hezbollah, and their agents and proxies to support and commit acts of international terrorism, and yet continued to provide that assistance.

1350. Each Defendant provided substantial assistance to the Iranian entities for at least several years.

1351. Each Defendant's assistance was therefore deliberate and long-term, not a passing fancy or impetuous act.

1352. Funding of the IRGC and Hezbollah and the terrorist attacks that they and their agents and proxies committed were the natural and foreseeable consequences, and foreseeable risk, of laundering billions of dollars clandestinely through the United States on behalf of a State

Sponsor of Terrorism in order to conceal these activities from U.S. regulators, law enforcement and counter-terrorist financing authorities.

1353. Plaintiffs' injuries were proximately caused by the IRGC's and Hezbollah's acts of international terrorism.

TENTH CLAIM FOR RELIEF

COMMERZBANK'S CIVIL LIABILITY FOR AIDING AND ABETTING IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (JASTA)

1354. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1355. Defendant Commerzbank knowingly provided substantial assistance to Hezbollah through Hezbollah's Martyrs Foundation in Lebanon.

1356. Defendant Commerzbank was generally aware that by providing material support to Hezbollah through the Martyrs Foundation, it played a role in giving Hezbollah, directly or indirectly, access to the international financial system that allowed the terrorist organization to effectively raise funds from donors outside of Lebanon.

1357. The nature of the act assisted, illegally laundering material support for the Martyrs Foundation through the United States, heavily depended on the active and sustained cooperation of Defendant Commerzbank, which was one of the largest dollar-clearing banks in the world.

1358. The assistance Defendant Commerzbank provided was substantial.

1359. Defendant Commerzbank knew or was deliberately indifferent to Hezbollah's unlawful acts (acts of international terrorism, which are particularly offensive acts), and yet continued to provide it assistance.

1360. Defendant Commerzbank assisted Hezbollah for several years.

1361. Terrorists attacks were the natural and foreseeable consequences, and foreseeable risk of Defendant Commerzbank's substantial assistance to Hezbollah.

ELEVENTH CLAIM FOR RELIEF

BANK SADERAT PLC'S CIVIL LIABILITY FOR AIDING AND ABETTING IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (JASTA)

1362. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1363. Defendant Bank Saderat Plc substantially assisted Hezbollah by knowingly providing it material support.

1364. Defendant Bank Saderat Plc knew that, or exhibited deliberate indifference as to whether, providing material support to Hezbollah raised a substantial probability that the funds it provided, and the sources of material support which it concealed and disguised, would be used to benefit Hezbollah and its agents and increase Hezbollah's capacity to engage in terrorist activities and acts of international terrorism.

1365. Defendant Bank Saderat Plc was generally aware that by providing, and concealing and disguising the source of, material support for Hezbollah, it played a role in giving Hezbollah, directly or indirectly, access to the U.S. and international financial system that allowed the terrorist organization to fund its terrorist activities.

1366. The nature of the acts assisted, which were both the funding of Hezbollah and Hezbollah's acts of international terrorism, including providing weapons for and directing attacks on American service members, aid workers, private contractors and journalists and the attacks themselves, benefited from and were virtually dependent on access to vast amounts of U.S. dollars.

1367. The amount of assistance Defendant Bank Saderat Plc provided—millions of dollars illegally transferred to Hezbollah and access to the U.S. financial system while blinding

U.S. counter-terror finance authorities—was integral to the acts of terrorism at issue.

1368. Defendant Bank Saderat Plc had an extremely close relationship with, and was a fundraising conduit of, Hezbollah.

1369. Defendant Bank Saderat Plc knew or was deliberately indifferent to Hezbollah's unlawful acts (acts of international terrorism, which are particularly offensive acts), and yet continued to provide it assistance.

1370. Defendant Bank Saderat Plc assisted Hezbollah for several years.

1371. Terrorist attacks were the natural and foreseeable consequences, and foreseeable risk, of Defendant Bank Saderat Plc's substantial assistance to Hezbollah.

TWELFTH CLAIM FOR RELIEF

STANDARD CHARTERED BANK'S, CREDIT SUISSE'S, AND HSBC'S CIVIL LIABILITY FOR AIDING AND ABETTING IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (JASTA)

1372. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

1373. Defendants SCB and Credit Suisse knowingly provided substantial assistance to the IRGC and Hezbollah by facilitating their acquisition of U.S.-origin export-controlled goods on behalf of, among others, Mahan Air and various sub-agencies of MODAFL.

1374. These controlled items include aircraft parts that enabled Mahan Air to transport IRGC and Hezbollah personnel, weapons, and funds into Iraq.

1375. Defendants SCB and HSBC provided material support to the IRGC through, *inter alia*, the IRGC's U.S.-designated agent NIOC.

1376. Defendant HSBC laundered Iranian funds for the CBI, Bank Saderat and Bank Melli knowing that U.S policymakers had "direct evidence against Bank Saderat particularly in

relation to the alleged funding of Hezbollah" and that they "suspected all major Iranian State owned banks of involvement in terrorist funding…."

1377. From the counter-terror and counter-WMD proliferations export control and financial sanctions they violated and from publicly available information, Defendants SCB and Credit Suisse knew that, or exhibited deliberate indifference as to whether, the IRGC and Hezbollah (and their agents, including NIOC and MODAFL) would use, or with a substantial probability would use, those export-controlled items and illegal access to the U.S. financial system (including concealment of material support) to increase their capacity to commit acts of international terrorism in Iraq.

1378. The nature of the acts encouraged and assisted, included providing illegal access to the U.S. financial system and export-controlled items, heavily depended on Defendants SCB, Credit Suisse, and HSBC's illegal assistance (which were among the largest dollar-clearing banks in the world).

1379. The amount of assistance Defendants SCB, Credit Suisse, and HSBC provided—access to export-controlled items and billions of dollars illegally transferred to NIOC and other IRGC entities so as to blind U.S. counter-terror finance authorities—was integral to the acts of terrorism at issue.

1380. Defendants SCB, Credit Suisse, and HSBC had a close relationship with many of the Iranian entities in working out and maintaining the scheme, including exchanging secret communications in order to develop and constantly adjust methods for circumventing U.S. counter-terrorism controls.

1381. Defendants SCB, Credit Suisse, and HSBC knew or were deliberately indifferent to Iran's unlawful acts (acts of international terrorism, which are particularly offensive acts), and yet continued to provide that assistance.

1382. Defendants SCB, Credit Suisse, and HSBC assisted the IRGC, and other Iranian entities that were a part of its terror apparatus, for several years.

1383. Terrorists attacks were the natural and foreseeable consequences, and foreseeable risk, of Defendants SCB's, Credit Suisse's, and HSBC's substantial assistance to the IRGC and its acquisition of U.S.-origin export-controlled goods on behalf of, among others, Mahan Air and various sub-agencies of MODAFL.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

(a) Accept jurisdiction over this action;

(b) Enter judgment against Defendants and in favor of Plaintiffs for compensatory damages in amounts to be determined at trial;

(c) Enter judgment against Defendants and in favor of Plaintiffs for treble damages pursuant to 18 U.S.C. § 2333(a);

(d) Enter judgment against Defendants and in favor of Plaintiffs for any and all costs sustained in connection with the prosecution of this action, including attorneys' fees, pursuant to 18 U.S.C. § 2333(a);

(e) Enter an Order declaring that Defendants have violated the Anti-Terrorism Act, 18 U.S.C. § 2331 *et seq*.; and

(f) Grant such other and further relief as justice requires.

PLAINTIFFS DEMAND A TRIAL BY JURY ON ALL ISSUES SO TRIABLE.

Dated: December 20, 2019

By /s/ Gary M. Osen

Gary M. Osen
Cindy Schlanger
Peter Raven-Hansen, Of Counsel
Ari Ungar
Aaron Schlanger
Michael Radine
OSEN LLC
2 University Plaza, Suite 402
Hackensack, NJ 07601
(201) 265-6400
(201) 265-0303 Fax

1441 Broadway, Suite 6022
New York, New York 10018
(212) 354-0111

TURNER & ASSOCIATES, P.A.
C. Tab Turner
4705 Somers Avenue, Suite 100
North Little Rock, AR 72116
(501) 791-2277

Attorneys for Plaintiffs