

18-1031

---

---

IN THE  
**United States Court of Appeals**  
FOR THE SEVENTH CIRCUIT

---

---

RHONDA KEMPER,

*Plaintiff-Appellant,*

— v. —

DEUTSCHE BANK AG,

*Defendant-Appellee.*

---

ON APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ILLINOIS  
CIVIL DIVISION  
NO. 3:16-CV-00497-MJR-SCW  
HONORABLE MICHAEL J. REAGAN

---

**JOINT APPENDIX**

---

TROY A. BOZARTH  
HEPLER BROOM, LLC  
130 North Main Street  
P.O. Box 510  
Edwardsville, Illinois 62025  
(618) 656-0184

JOHN E. HALL  
DAVID M. ZIONTS  
COVINGTON & BURLING LLP  
One City Center  
850 Tenth Street, N.W.  
Washington, DC 20001  
(202) 662-6000

*Attorneys for Defendant-Appellee*

PETER RAVEN-HANSEN  
GARY M. OSEN  
OSEN LLC  
2 University Plaza, Suite 402  
Hackensack, New Jersey 07601  
(201) 265-6400

*Attorneys for Plaintiff-Appellant*

---

---

**TABLE OF CONTENTS**

	PAGE
Complaint (Dkt. No. 1, filed May 4, 2016) .....	JA1
Exhibit A to Complaint (Dkt. No. 1-1, filed May 4, 2016) .....	JA59

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ILLINOIS

CHARLES J. SHAFFER, CHARLES L. )  
SHAFFER, JR., RHONDA KEMPER )  
 )  
Plaintiffs, )  
 )  
v. )  
 )  
DEUTSCHE BANK AG )  
 )  
Defendant. )

Case No.: 3:16-cv-497

**JURY TRIAL DEMANDED**

**COMPLAINT**

Plaintiffs, CHARLES J. SHAFFER, CHARLES L. SHAFFER, JR., and RHONDA KEMPER, submit the following Complaint:

**I. NATURE OF THE ACTION**

1. This is a civil action under 18 U.S.C. § 2333(a) of the Anti-Terrorism Act (“ATA”) by American nationals for treble damages against Deutsche Bank AG, an international bank that knowingly conspired with, *inter alia*, the Islamic Republic of Iran (“Iran”) and its banking agents (including Bank Saderat, Bank Melli and Iran’s Central Bank) (the “Conspiracy”) from at least 1999 to 2011 to evade U.S. economic sanctions and disguise financial payments, thereby foreseeably enabling Iran’s involvement in the terrorist acts that injured the Plaintiffs.

2. Defendant committed acts of international terrorism by violating 18 U.S.C. § 2339A and § 2339B knowing, or being deliberately indifferent to the fact, that Iran would foreseeably use some of the funds it laundered through the United States to finance the U.S.-designated Foreign Terrorist Organization Hezbollah; the U.S.-designated Islamic Revolutionary Guard Corps (“IRGC”), and its lethal subdivision 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 occasionally referred to herein collectively as “Special Groups”) that killed, injured, or maimed American nationals serving as part of the Coalition Forces’ peacekeeping efforts in Iraq from 2004 to 2011, including the Plaintiffs and/or their families.

3. The Plaintiffs are Charles James Shaffer, who was severely wounded by Iranian agents in Iraq, and his father, Charles L. Shaffer, Jr.; and Rhonda Kemper, the mother of David Schaefer, who was killed by Iranian-manufactured munitions in Iraq.

4. The Plaintiffs seek to hold Defendant legally accountable for its integral role in helping Iran finance, orchestrate, and support terrorist attacks on U.S. peacekeeping forces in Iraq from 2004 to 2011.

5. During that period, Iran needed billions of U.S. dollars to conduct a protracted terror campaign claiming the lives of at least hundreds of Americans while simultaneously trying to complete a clandestine Weapons of Mass Destruction program that required billions of U.S. dollars.

6. For Iran this was especially true 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.

7. During the last decade prior to the implementation of the Joint Comprehensive Plan of Action (signed on July 14, 2015), Iran therefore intensified its efforts to access the U.S. financial system while simultaneously evading U.S. sanctions intended to circumscribe its access.

8. Fortunately for Iran, despite ever-intensifying efforts over the prior decade by the United States, European Union and United Nations to isolate it and restrict its capacity to fund

terrorism and obtain Weapons of Mass Destruction, Defendant Deutsche Bank and other Western financial institutions knowingly provided essential assistance for Iran's illegal scheme.

## II. JURISDICTION AND VENUE

9. This Court has exclusive 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 nationals of the United States and/or their estates, survivors, or heirs, who have been injured by reason of acts of international terrorism.

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

11. Defendant is subject to personal jurisdiction in the United States pursuant to 18 U.S.C. § 2334(a) and Fed. R. Civ. P. 4(k)(1)-(2). Defendant's unlawful conduct was purposefully directed at the United States, and the Conspiracy was specifically designed to – and did – effectuate the flow of billions of U.S. dollars through the United States in violation of U.S. laws.

## III. THE PLAINTIFFS

### 1. THE SEPTEMBER 1, 2008 ATTACK – MOSUL

#### The Shaffer Family

12. Plaintiff Charles James Shaffer is a citizen of the United States and domiciled in the State of Illinois, County of St. Clair.

13. On September 1, 2008, Charles James Shaffer, then age 23, was serving in the U.S. military in Iraq as part of the U.S. peacekeeping mission authorized by the U.N. Security Council in October 2003 to maintain "security and stability." S.C. Res. 1511, para. 13, U.N. Doc. S/RES/1511 (Oct. 16, 2003).

14. Mr. Shaffer was on routine patrol in Mosul when his vehicle was struck by an

Iranian-manufactured Improvised Explosive Device (“IED”) known as an Explosively Formed Penetrator (“EFP”) provided to Iranian-funded and -trained terror operatives in Iraq.

15. As a result of the attack, he sustained injuries that included second degree burns to his face and hands, significant loss of blood, and damage to his right leg.

16. The injuries necessitated an above-the-knee amputation of Mr. Shaffer’s right leg.

17. He was placed in a medically-induced coma for four days.

18. Mr. Shaffer was initially treated in Iraq and subsequently received treatment in Germany, primarily to prepare him for travel and treatment at Walter Reed Hospital in the United States. He remained at Walter Reed Hospital through August 2010.

19. Initially, Mr. Shaffer underwent surgeries every few days, for weeks, to address infection, treat the amputation site, and attend to the remaining limb. Multiple procedures were also performed to address and repair the affected area.

20. The second-degree burns required laser treatment to his face to address the discoloration that had resulted.

21. Mr. Shaffer has also experienced “phantom limb” pain and sensations.

22. Mr. Shaffer has been diagnosed with Post-Traumatic Stress Disorder (“PTSD”) and Traumatic Brain Injury (“TBI”) and experiences memory loss. He has been prescribed medication to address the symptoms of these conditions and emotional impact of the attack.

23. Mr. Shaffer continues to experience pain and emotional distress daily, and he has received and continues to receive treatment for his injuries.

24. As a result of the attack, and the injuries he suffered, Charles James Shaffer has experienced severe physical and mental anguish and extreme emotional pain and suffering.

25. Plaintiff Charles L. Shaffer, Jr. is a citizen of the United States and domiciled in

the State of Illinois, County of St. Clair. He is the father of Charles James Shaffer.

26. As a result of the attack, and the injuries Charles James Shaffer suffered, Plaintiff Charles L. Shaffer, Jr. has experienced severe mental anguish and extreme emotional pain and suffering.

**2. THE MAY 16, 2009 ATTACK - BASRA**

**The Schaefer Family**

27. David Schaefer was a citizen of the United States and domiciled in the State of Illinois, County of St. Clair, when he was killed in Iraq.

28. On May 16, 2009, David Schaefer, aged 27, was serving in the United States military in Iraq as part of the aforementioned U.S. peacekeeping mission when an Iranian-manufactured EFP provided to Iranian-funded and -trained terror operatives in Iraq detonated near his unit.

29. David Schaefer was killed in the attack.

30. Plaintiff Rhonda Kemper is a citizen of the United States and domiciled in the State of Illinois, County of Randolph. She is the mother of David Schaefer.

31. As a result of the attack, and the death of David Schaefer, Plaintiff Rhonda Kemper has experienced severe mental anguish, extreme emotional pain and suffering, and loss of her son's society, companionship, comfort, advice and counsel.

**3. BOTH OF THE ATTACKS AT ISSUE IN THIS COMPLAINT WERE ACTS OF INTERNATIONAL TERRORISM**

32. 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.

33. At no time relevant to this action did the United States engage in an armed conflict with the military forces of Iran, or did Iran's military forces or their agents engage in

lawful acts of war against Coalition Forces.

34. At no time relevant to this action, did the operatives of Hezbollah, the IRGC, the IRGC-QF and the Special Groups who killed and injured Coalition Forces and civilians in Iraq 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.

35. The specific attacks alleged herein were all carried out by terrorists and terrorist organizations and entities like Hezbollah and the Special Groups, not by armed forces of recognized governments or military forces.

36. The injuries the Plaintiffs sustained were not the result of, or in the course of, a declared war with Iran, or armed conflict between the United States and Iran.

37. The conduct of Iran, the IRGC, IRGC-QF, Hezbollah, and the Special Groups violated the laws of armed conflict, and the attacks upon Iraqi and other civilians constituted a substantial, rather than an incidental, part of their objectives and conduct.

38. The acts of the IRGC, IRGC-QF, Hezbollah, and/or the Special Groups 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 also were acts engaging in 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.

#### IV. THE DEFENDANT

39. Defendant Deutsche Bank AG, a global investment bank, has a presence in more than 70 countries, with more than 2,700 branches worldwide.



40. It is organized under the laws of, and headquartered in, Germany, and its principal office is in Frankfurt.

41. It has more than 98,000 employees, and its total assets exceed \$1.9 trillion.

42. Defendant's services encompass investment, corporate and retail banking, as well as asset and wealth management.

43. Defendant operates a branch in New York State that is licensed, supervised, and regulated by the New York State Department of Financial Services (the "DFS").

44. Defendant also has a U.S. subsidiary, Deutsche Bank Trust Company Americas ("DBTCA"), which 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.

45. Deutsche Bank employed both its New York branch and U.S. subsidiary in the commission of the offenses that give rise to this action.

## V. FACTUAL ALLEGATIONS

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

46. 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.

47. The United States officially designated Iran as 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. That designation has remained in force throughout the relevant time period to this action.

48. Since its 1984 designation until the implementation of the Joint Comprehensive

Plan of Action (signed on July 14, 2015), the United States attempted to constrain and deter Iran's sponsorship and conduct 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. dollars, for Iran's support of such activities.

49. The United States designated Iran's proxy, Hezbollah,<sup>1</sup> as a Foreign Terrorist Organization ("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.

**B. IRAN'S AGENTS, HEZBOLLAH AND THE IRGC, FOMENT TERRORISM IN IRAQ**

50. 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.

51. Through Hezbollah, Iran: orchestrated a series of kidnappings of Westerners in Lebanon, including several Americans, in the 1980s; killed more than two hundred U.S. Marines at their barracks in Beirut, Lebanon, in 1983; hijacked TWA flight 847 in 1985; and launched two major 1990s attacks on Jewish targets in Argentina – the 1992 bombing of the Israeli Embassy (killing twenty-nine) and the 1994 bombing of a Jewish community center (killing eighty five).

---

<sup>1</sup> The 2007 U.S. State Department's Country Reports on Terrorism noted, "The [Islamic Revolutionary Guard Corps-] Qods Force has a long history of supporting Hezbollah, providing it with guidance, funding, weapons, intelligence, and logistical support. The Qods Force operates training camps for Hezbollah in Lebanon's Bekaa Valley and has reportedly trained more than 3,000 Hezbollah fighters at IRGC training facilities in Iran. The Qods Force provides roughly \$100 to \$200 million in funding a year to Hezbollah and has assisted Hezbollah in rearming." The report further noted that Hezbollah "receives training, weapons, and explosives, as well as political, diplomatic, and organizational aid from Iran."

52. As a result of its mission, conduct, and terrorist activities, Hezbollah was designated a Specially Designated Terrorist (“SDT”) by the United States on January 25, 1995.

53. On October 8, 1997, Hezbollah was designated an FTO by the United States. As noted above, it has retained that designation since that time.

54. On October 31, 2001, pursuant to E.O. 13224, Hezbollah was designated a Specially Designated Global Terrorist (“SDGT”) by the United States.

55. For more than 30 years, Iran, through the IRGC, has funded, trained and equipped Hezbollah.

56. The IRGC-QF’s “Department 2000” manages Iran’s relationship with Hezbollah, which includes the flow of some of Iran’s most sophisticated weapon systems, including military grade EFPs, anti-tank guided missiles (“ATGMs”), and various rockets, such as the Fajr-5.

57. Beginning with the 2003 U.S. overthrow of Saddam Hussein’s regime in Iraq, Iran has assiduously worked to expand its influence in Iraq and throughout the region in a variety of ways, including fomenting violence and terrorism when such activities have served its ambitions.

58. In doing so, it has relied on both Hezbollah and the IRGC.

59. According to a December 20, 2004 *Washington Post* article, “Western diplomats and political analysts in Beirut estimated that Hezbollah received \$200 million a year from Iran.”

60. Sometime after the 2003 U.S. invasion of Iraq, Hezbollah created “Unit 3800,” an entity dedicated to supporting Iraqi Shi’a terrorist groups targeting Multi National Forces in Iraq (“MNF-I”).

61. Unit 3800 was established by Hezbollah leader Hassan Nasrallah at Iran’s request.

62. Unit 3800 has trained and advised various Shi’a militias in Iraq, later termed

“Special Groups.”

63. Hezbollah training camps in southern Lebanon and Iran, and Hezbollah’s expertise in the use of EFPs, kidnapping, communications and small-unit operations, were critical to the IRGC’s operations in Iraq between 2004 and 2011.

64. Iran’s support of terrorist groups in Iraq was described in the 2005 U.S. State Department’s Country Reports on Terrorism, which observed: “Iran has provided political and ideological support for several terrorist and militant groups active in Iraq. Attractive to terrorists in part because of the limited presence of the United States and other Western governments there, Iran is also a safe haven in that known terrorists, extremists, and sympathizers are able to transit its territory and cross the long and porous border into Iraq. Iran also equips terrorists with technology and provides training in extremist ideology and militant techniques.”

65. The IRGC’s subversion of Iraq has not been limited to terrorism. The IRGC has also infiltrated Iraqi society, providing “political and ideological support” via purportedly charitable associations such as Khomeini Social Help Committee – in Karbala, Najaf, Kut, and Sadr City – and the Imam Mohammad Bagher Institute in Najaf.

66. The IRGC also purchased or developed 7 television stations and at least 3 radio stations in Iraq.

67. All of these “investments” required substantial funding in U.S. dollars (as Iraqi local currency was not widely accepted in Iraq during this time period).

68. According to the same U.S. State Department’s 2005 Country Reports on Terrorism: “[t]he IRGC was increasingly involved in supplying lethal assistance to Iraqi militant groups, which destabilizes Iraq ... Senior Iraqi officials have publicly expressed concern over

Iranian interference in Iraq, and there were reports that Iran provided funding, safe passage, and arms to insurgent elements.”

69. By early 2005, the presence of Hezbollah operatives in Iraq became an open secret when Iraqi interior minister Falah al-Naqib announced the arrest of eighteen Lebanese Hezbollah members on terrorism charges.

70. Two years later, according to U.S. intelligence estimates, following the 2007 arrest of Hezbollah’s senior operative in Iraq, the IRGC-QF provided Hezbollah and one of its local trainers, Ali Musa Daqduq, up to \$3 million in U.S. currency every *month*.

71. In October 2007, the IRGC-QF was designated as an SDGT pursuant to E.O. 13324 for its terrorism-related activities. The U.S. Treasury Department’s press release announcing the designation noted 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.)*

72. In 2008, Pentagon Press Secretary Geoff Morrell reported on the “smuggling system -- in which the Iranians are providing their allies within Iraq, these special groups, with the munitions that are then used to take on us, whether it be EFPs or rockets or conventional arms. These are being used by these special groups and being provided by the Iranians.”

73. According to a 2010 report by the Combatting Terrorism Center at West Point,

Iran pays Iraqi “insurgent” groups “between \$4,000 and \$13,000 per rocket or roadside bomb, depending on the circumstances.”

74. Because of the perceived unreliability and value of the post-Hussein regime Iraqi currency, Special Groups in Iraq (like most people in Iraq) used U.S. currency almost exclusively.

75. According to Brigadier Gen. Kevin J. Bergner, a U.S. military spokesman, “the Qods Force has provided armor-piercing weapons to extremist groups in Iraq, funneling them up to \$3 million a month and training Iraqi militiamen at three camps near Tehran.”

76. General Bergner added, “[t]he Iranian Qods Force is using Lebanese Hezbollah essentially as a proxy, as a surrogate in Iraq ... Our intelligence reveals that senior leadership in Iran is aware of this activity.”

77. On January 9, 2008, the U.S. Treasury Department designated four individuals and one entity under E.O. 13438 for threatening the peace and stability of Iraq and the government of Iraq. Three of the individuals, Ahmed Foruzandeh (a Brigadier General in the IRGC-QF), Abu Mustafa Al-Sheibani, and Isma’il Hafiz Al Lami (a/k/a “Abu Dura”) were all based in Iran and/or received funding from Iran.

78. Regarding Abu Mustafa Al-Sheibani, the Treasury Department press release stated:

Iran-based Abu Mustafa Al-Sheibani leads a network of Shia extremists that commit and provide logistical and material support for acts of violence that threaten the peace and stability of Iraq and the Government of Iraq. Al-Sheibani’s Iran-sponsored network was created to affect the Iraqi political process in Iran’s favor. 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.*

Additionally, Al-Sheibani commands several pro-Iranian insurgent groups in southern Iraq that work to destabilize Iraq and sabotage Coalition efforts. These groups use a variety of weapons, to include mortars, Katyusha rockets, and anti-tank landmines. *Ordered by IRGC headquarters to create disorder, the task of these groups is to attack bases of Coalition Forces in southern Iraq, particularly British forces. (Emphasis added.)*

79. To that end, Iran (with Hezbollah's aid) armed, trained, and funded a variety of Special Groups and infiltrated and co-opted Iraqi security forces in an effort to kill or maim Coalition Forces to coerce the United States into withdrawing them and terrorize its civilian population in order to increase Iran's own influence.

80. Iran's Defense Industries Organization ("DIO") (designated as a Specially Designated National ("SDN") by the U.S. on March 30, 2007) 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.

81. The DIO was also designated by the United Nations.

82. Weapons caches seized from Special Groups in Iraq included large quantities of weapons produced by Iran in 2006 and 2007, including 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.

83. According to the U.S. State Department, the DIO used Bank Melli in Hamburg to receive payments and to transfer funds.

84. Bank Melli was an active participant in the Conspiracy, and as detailed *infra*, it was designated an SDN in 2007.

C. **IRAN FUNDED THE DESIGN AND PRODUCTION OF EXPLOSIVELY FORMED PENETRATORS (“EFPS”) USED TO KILL OR MAIM COALITION FORCES, INCLUDING THE PLAINTIFFS.**

85. 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.

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

87. First used by Hezbollah against Israeli armor in Lebanon, EFPs are known as shaped charges, usually made with a manufactured concave copper disk and a High Explosive packed behind the liner.

88. In Iraq, EFPs were often triggered by a passive infra-red device that set off the explosion within the casing of the EFP, forcing the copper disk forward, turning it into a high velocity slug that could pierce most military-grade armor.

89. 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.

90. EFPs are far more sophisticated than homemade explosive devices such as traditional IEDs, and they are designed specifically to target vehicles such as armored patrols and



supply convoys, though Hezbollah and the Special Groups have deployed them against U.S. and Iraqi civilians also.

91. In 2006, the U.S. State Department's 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: "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 Hizballah. The Iranian Revolutionary Guard was linked to armor-piercing explosives that resulted in the deaths of Coalition Forces. The Revolutionary Guard, along with Lebanese Hizballah, 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.)

92. Also in 2006, Brigadier Gen. Michael Barbero, Deputy Chief of Staff for Strategic Operations of the Multi-National Force – Iraq 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."

93. That same year, the Deputy Chief of Staff for Intelligence with the MNF-I, U.S. Army Major General Richard Zahner, declared that "[l]abels 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."

94. Major General Zahner further added: “the 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.”

95. General Bergner commented on Iran funding Hezbollah operatives in Iraq: “[a]ctions 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.”

96. Bergner further commented: “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.”

97. In May 2007, the Commander of the Multinational Division-Center, U.S. Army Major General Richard Lynch, commented that “[m]ost 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.)

98. 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.

99. 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.

100. These observations continued in 2008. 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.

101. Likewise, the U.S. 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.

102. Similarly, in 2011, the U.S. Ambassador to Iraq, James F. Jeffrey, was quoted saying: "fresh 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."

103. 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 the Central Bank of Iran, Bank Melli and Bank Saderat) on behalf of and for the benefit of the IRGC, Hezbollah and the Islamic Republic of Iran

Shipping Lines (“IRISL”)<sup>2</sup> – an Iranian entity that transported components of the EFPs and provided other logistical support for the attacks – as part of the Conspiracy set forth in detail herein.

104. Moreover, although both Iran and Hezbollah utilized a variety of means to raise and transport U.S. dollars, because of the size and scope of Iran’s efforts to murder Americans in Iraq and subvert the U.S.-sponsored and freely elected government in Iraq, Iran required access to hundreds of millions of dollars that could only be reliably and effectively transferred through the global financial system with the illicit assistance of several Western financial institutions, including Defendant.

105. U.S. “dollar clearing” – primarily (in this case) through the Clearing House Interbank Payments System or “CHIPS” system – is an elaborate intra-bank system in the U.S. by which banks settle the credits and debits on their accounts with other banks all across the globe on a daily basis.

106. The U.S. “dollar clearing” system is not only critical to the workings of the global economy, but also provides financial institutions (and states) with critical, essential access to global trade and credit in U.S. dollars.

107. Thus, once Iran gained clandestine access to the U.S. “dollar clearing” system it could not only launder billions of dollars in funds transfers, but it could also borrow against the funds it held with Defendant – facilitating further undetected transactions around the world in U.S. dollars – for both ordinary commercial purposes and the illegal aims and objectives of the Conspiracy.

108. This broad-based access to the U.S. “dollar clearing” system was essential to Iran

---

<sup>2</sup> IRISL, a/k/a IRI Shipping Lines, ARYA Shipping Company, is Iran’s national maritime carrier: a global operator 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.

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.

109. Iran's objectives were not secret. Its pursuit of Weapons of Mass Destruction was 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.

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

111. 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. 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.)*

112. The BBC followed up with multiple reports in 2006 describing military briefings on Iranian material support to Shi'a groups targeting British and U.S. forces. 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.

113. In another example, on September 26, 2008 CNN reported that U.S. officials claimed Iran had provided Shi’a militia in Iraq with “millions of dollars” 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.”

#### D. U.S. SANCTIONS AND IRAN’S RELIANCE ON U.S. DOLLARS

114. 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. It was soon established that the IRGC had trained and equipped the operatives responsible for the bombing.

115. 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.)

116. To ensure that U.S. financial institutions that process international wire transfers 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 to monitor and screen all wire transfer activities. Banks in New York that process most of the world's U.S. dollar payments 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, 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.

117. At the same time, because, on average, 60 percent of Iranian government revenues and 90 percent of export revenues originate from oil and gas resources, a market largely denominated in U.S. dollars (known as "petrodollars"<sup>3</sup>), and because Iran's currency, the Rial, has (in part due to U.S. sanctions) remained one of the world's least valued currencies, the Iranian regime has been desperately dependent on access to U.S. dollars.

118. Thus, reliably consistent access to, and the ability to facilitate trade in, U.S. dollars has been critical and essential to the Iranian regime's capacity to fund its terror proxies such as Hezbollah in Lebanon and to fuel its other terrorism and weapons proliferation activities through the IRGC.

119. The importance of funding Hezbollah, the IRGC and later, Kata'ib Hezbollah<sup>4</sup> and other Special Groups became even more acute for Iran after the 2003 U.S. invasion of Iraq. After that event, Iran directed Hezbollah to create "Unit 3800" (¶ 60 *et seq.*) and began devoting

---

<sup>3</sup> Because the United States was the largest producer and consumer of oil in the world, the world oil market had been priced in U.S. dollars since the end of World War II.

<sup>4</sup> Kata'ib Hezbollah was designated an FTO on June 24, 2009.



increasing financial resources to gain influence in Iraq, inflict casualties on American citizens in Iraq, and intensify its quest for Weapons of Mass Destruction.

120. *None* of these goals could be accomplished without U.S. currency, access to the international financial system, and the agreement of Western financial institutions, including Defendant, to shield Iran's unlawful activities from detection.

E. THE U-TURN EXEMPTION AND ITS REVOCATION

121. Notwithstanding broad sanctions against Iran and specific sanctions against certain Iranian banks, the United States government permitted Iran 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), while insisting on careful monitoring of all Iranian transactions to both deter and detect terror financing and weapons proliferation activities. The purpose of the U-Turn exemption was to provide Iranian parties indirect access to U.S. dollar transactions for legitimate agencies, operations, and programs, *provided* they were fully disclosed and not earmarked for terrorist or other illegitimate and illegal purposes.

122. 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*: (1) 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; (2) none of the parties to the transactions had been designated an SDN; and (3) the transaction was not for an SDN's benefit.

123. The U-Turn exemption was therefore conditioned on transparency to permit careful monitoring of all Iranian transactions to both deter and detect terror financing and weapons proliferation activities. Because so much of Iran’s international trade has historically flowed through the United States in U.S. dollars, and because Iran’s primary terrorist proxy, Hezbollah, operates in Lebanon (itself a dollarized economy, largely dependent on U.S. currency), maintaining transparency in the processing of Iranian U.S. dollar transactions has been a vital part of the architecture of U.S. national security for decades and was reflected in the Iranian Trade Regulations.

124. Iran’s access – through the U-Turn exemption – was intended to be closely monitored, including filtering all U-Turn exemption transactions through the sophisticated computer systems used by U.S. financial institutions to monitor and screen all wire transfers.

125. The U.S. authorities’ realization that Iran was engaging in “deceptive banking practices” led it to target key Iranian financial institutions, entities, and individuals under proliferation, terrorism, and Iraq-related authorities, i.e., E.O. 13382, E.O. 13224, and E.O. 13438, respectively.

126. The U.S. authorities also recognized the necessary and essential knowing participation of Western financial institutions, including Defendant, in Iran’s “deceptive banking practices,” as set forth in this Complaint.

127. Despite Iran’s feeble economy during the entire relevant period of time, its oil exports still provided the regime with revenues in U.S. dollars through, among others, the National Iranian Oil Company (“NIOC,” which was later designated an SDN pursuant to E.O. 13382 and identified as an agent or affiliate of the IRGC) and the Central Bank of Iran.

128. The challenge Iran faced was that it was almost entirely dependent on U.S. dollars, but U.S. sanctions and the attendant monitoring of Iran's financial activities were incompatible with Iran's terror financing and Weapons of Mass Destruction proliferation goals.

129. Moreover, between 2004 and 2011, both Lebanon (where Iran's agent, Hezbollah is based) and Iraq (where Iran's proxies were launching terror attacks) were U.S.-dollarized economies, and funding Iran's terror proxies was a highly "dollar-sensitive" endeavor.

130. To free itself from U.S. sanctions and the attendant monitoring of its financial activities, Iran needed the active assistance of at least *several* of the world's *largest* (non-U.S.) banks that were already accustomed to large volumes of dollar clearing and thus would be less likely to raise suspicions among Western financial institutions to assist its illegal goals.

131. In the spring of 2006, the Manhattan District Attorney's Office first discovered evidence of the Conspiracy engaged in by certain Western financial institutions (including Defendant herein) on behalf of and in conjunction with Iran and Iranian banks.

132. As the New York State Department of Financial Services 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.)

133. These findings led to a wide-ranging investigation that ultimately resulted in the entry of a series of Deferred Prosecution Agreements with several Western financial institutions (as well as a Japanese financial institution), and it exposed the vulnerability of America's terror

financing security architecture inherent in the U-Turn exemption, because foreign banks, including Defendant herein, were conspiring with Iran to help it evade U.S. sanctions and secrete hundreds of billions of dollars through the U.S. financial system.

134. Based on figures from the International Monetary Fund and the Central Bank of Iran, from 2004 through 2011 Iran's total revenues from oil and natural gas sales totaled approximately \$972.9 Billion.

135. Without the Conspiracy involving foreign financial institutions, including Defendant, Iran could not have transferred the volume of U.S. dollars it did for the benefit of Hezbollah and the IRGC through the international financial system. Nor could it have exploited the U-Turn exemption to blind U.S. regulators and law enforcement to the degree and for the duration that it did.

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

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

138. In revoking the U-Turn exemption, the U.S. government 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.

## VI. THE CONSPIRACY

139. As noted above, as used in this Complaint, "the Conspiracy" refers to an illegal criminal agreement and scheme among, *inter alia*, Iran, the IRGC, several Iranian banks including Bank Saderat, Bank Melli and CBI (referred to herein collectively as the "Iranian Bank Co-conspirators"), IRISL, and various Western financial institutions, including Defendant.

140. The Conspiracy began no later than 1987, and Defendant joined it in 1999 and actively participated in it during the relevant time period. On information and belief, the Conspiracy continues through the present day.

141. The aims and objectives of the Conspiracy (which followed Iran's designation as a State Sponsor of Terrorism in 1984 and the sanctions subsequently imposed upon it) all of which were foreseeable to Defendant, and which Defendant knew or was deliberately indifferent to, included, among others:

- a. Concealing Iran's 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 U.S. dollars for the benefit of Hezbollah;
- c. Facilitating illicit transactions totaling at least \$100 million U.S. dollars for the benefit of the IRGC and Bank Saderat, and other U.S. Specially Designated Nationals ("SDNs") (such as, as alleged below, Iranian Bank Co-conspirator Bank Melli Iran);
- d. Facilitating at least hundreds of illicit transactions on behalf of IRISL totaling more than \$60 million, including over 150 "stripped" transactions after IRISL was designated an SDN; and
- e. Enabling Iran, the Iranian Bank Co-conspirators (including Bank Saderat Plc), Hezbollah, and 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.

142. As part of the Conspiracy, Defendant knowingly and criminally agreed to alter, falsify, or omit information from payment messages that involved Iran or Iranian parties, including the Iranian Bank Co-conspirators and IRISL, which serve as financial conduits for the U.S.-designated terrorist entities IRGC-QF and Hezbollah, which organized and conducted the terrorist attacks on Coalition Forces, including those that injured the Plaintiffs.

143. Although the Conspiracy was effectuated in a variety of ways, Defendant, acting in concert with Iran, the Iranian Bank Co-conspirators and IRISL employed two primary techniques:

- a. Defendant 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 messages sent through U.S. correspondent banks – a practice commonly known and referred to as “stripping” transactions; and
- b. Defendant converted ordinary transactions involving SWIFT “MT 103” payment messages (that would disclose the details of the counter-parties to the transactions) into bank-to-bank transfers known as SWIFT “MT 202” payment messages (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.<sup>5</sup>

---

<sup>5</sup> When a bank customer sends an international wire payment, the de facto standard to execute payment is the MT103 SWIFT message (also called a serial payment, or a serial MT103 payment). When a financial institution sends a bank-to-bank credit transfer, the de facto standard to execute payment is the MT202 SWIFT message. The crucial difference, during the relevant time period, was that MT202 payments typically did not require the bank to identify the originating party to the transactions, and banks typically did not include that information in MT202 messages. A “cover payment” typically involves both types of messages: an MT103 message identifying all parties to the transaction was sent from the originating bank to the beneficiary, but the funds were transferred through the United States via an MT202 message that lacked that information. Instead of using MT103 payment messages for transactions involving the Iranian co-conspirators, which would have revealed the identity of the ordering customer and beneficiary to the bank clearing dollars in the U.S., Defendant often used MT202 “cover payment” messages for these bank-to-bank credit transfers, which did not identify the ordering customer and beneficiary.

144. For example, a November 2008 U.S. diplomatic cable noted: “When processing the transactions for the IRGC and IRGC-QF, Bank Melli requested that its name be removed from financial transactions.”

145. Absent Defendant’s criminal collusion and conspiratorial conduct, Iran and its agents, including the IRGC, IRISL, Bank Melli, Bank Saderat and the CBI could not have successfully hidden the volume of financial transactions that they succeeded in illegally clearing through the United States in U.S. dollars.

146. The connection between the IRGC, IRGC-QF and Bank Melli, their “deceptive banking practices” and the attacks 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.)*

147. Defendant knew about the existence of the Conspiracy, directly conspired with Iran through Bank Saderat, Bank Melli, the Central Bank of Iran and others, to facilitate the Conspiracy, took affirmative, extensive, and unlawful actions to facilitate the Conspiracy over long periods of time, and was aware of the existence and participation of other co-conspirators.

148. Defendant knew that Iran was a U.S.-designated State Sponsor of Terrorism at the time it agreed to join and actively take part in the Conspiracy, knew that Iran was clandestinely routing billions of dollars through the United States to hide its unlawful conduct, knew that this routing was not for legitimate agencies, operations, and programs of the Iranian government, and took affirmative steps to help Iran in its unlawful conduct.

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

150. Defendant also knew or was deliberately indifferent to the well-publicized fact that Iran and its terror proxies were killing and maiming 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.

151. Defendant also knew or was deliberately indifferent to the foreseeable (and almost 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 terrorism proxies that targeted American civilians and servicemen through acts of international terrorism in Iraq from 2004 to 2011.

152. Without Defendant's active participation in the Conspiracy, Iran could not have transferred the same volume of U.S. dollars to the IRGC and Hezbollah, nor could it have done so with the same ease and efficiency.

153. 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 Defendant's unlawful agreement to help Iran launder money through the United States.

154. As set forth below, Defendant altered, falsified, or omitted information from payment messages that it facilitated on behalf of Bank Saderat knowing, or deliberately



indifferent to the fact, that Bank Saderat was an SDGT that provided material support to Iran's terrorist activities.

155. As set forth below, Defendant was one of several banks that 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 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.

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

157. For example, an IRISL shipment of chemical weapons precursors from China was seized aboard the IRISL-flagged M/V Iran *Teyfour*, and a former Russian merchant ship, the *Monchegorsk*, flying a Cypriot flag, was seized with hidden cargo, including components for mortars and thousands of cases of powder, propellant, and shell casings for 125mm and 130mm guns.

158. 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, headed to Syria from Iran.

159. The vessel carried seven containers of small arms ammunition, as well as one container containing copper discs of the type used in EFPs to kill and maim the Plaintiffs herein.

160. The *Hansa India* was registered to the Hamburg-based shipping company Leonhardt & Blumberg, but had been under charter to Islamic Republic of Iran Shipping Lines for several years.

161. In November 2009, the Government of Israel intercepted an Islamic Republic of Iran Shipping Lines-flagged ship, the M/V *Francop* headed for Beirut, then Latakia, Syria with munitions crates stamped “IRISL” or including documentation marked with the IRGC-QF logo. The munitions included over two thousand 107mm “Katyusha” rockets, more than six hundred 122mm “Grad 20” rockets, various rocket fuses, mortar shells, rifle cartridges, fragment grenades and 7.62mm bullets.

162. The *Francop*, owned by the Cypriot shipping company UFS, was carrying containers clearly marked IRISL.

163. Defendant entered into its agreement with Iran and the Iranian Bank Co-conspirators (including Bank Saderat, Bank Melli and the CBI) aware that other co-conspirators were also actively participating in the Conspiracy, shared the common goal of the scheme’s purpose of providing Iran and the Iranian Bank Co-conspirators (including Bank Saderat, Bank Melli and the CBI) 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.

164. Accordingly, Defendant understood that its conduct was part of a larger scheme engineered by Iran; Defendant knew the participation of other conspirators was essential to the Conspiracy’s success; and Defendant knew of and joined in the overriding scheme and sought to achieve and facilitate a common goal of helping Iran to 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.

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

166. Despite that knowledge, Defendant knowingly conspired with Iran, and its agents (including Bank Saderat, Bank Melli and the CBI) 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 United States on behalf of Iran, IRISL, and the Iranian Bank Co-conspirators.

167. During the relevant time period, from 2004 to 2011, Defendant actively and knowingly 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, as set forth in greater detail herein.

168. Through the Conspiracy, Iran provided material support to Hezbollah, the IRGC and Special Groups that targeted American citizens in Iraq, and with substantial assistance from the Western financial institutions, including Defendant, it 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.

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

170. As part of the Conspiracy, Defendant took affirmative steps to violate U.S.

criminal laws and to conceal from U.S. depository institutions, law enforcement, and counter-terrorism agencies the flow of millions of U.S. dollars it was moving through the United States. This played a vital role in allowing Iran to secretly transfer millions of dollars for the benefit of the IRGC and Hezbollah, and through them to Kata'ib Hezbollah (itself an FTO) and other terrorist organizations actively engaged in murdering and maiming U.S. servicemen and civilians in Iraq.

171. Thus, for example, a State Department diplomatic cable from March 2008 noted: “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.”

172. In addition, absent the access to the U.S. “dollar clearing” system afforded by Defendant to Bank Saderat, both Iran’s and Hezbollah’s access to U.S. dollars would have been diminished, and Iran’s efforts to transfer large sums of U.S. dollars to Hezbollah would have been substantially impaired.

173. By knowingly agreeing to enter into the Conspiracy, by knowing or being deliberately indifferent to its lethal purposes, and by committing multiple overt acts in its

furtherance, Defendant provided Iran with the means to transfer more than \$150 million to the IRGC, Hezbollah and 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 injuries described herein.

174. 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, IRISL, the IRGC, Hezbollah, and/or Special Groups in committing the acts of international terrorism that injured the Plaintiffs 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.

175. 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, Defendant committed acts of international terrorism as defined by 18 U.S.C. §§ 2331, 2339A and 2339B that caused injury to the Plaintiffs, and is civilly liable under 18 U.S.C. § 2333(a) of the Anti-Terrorism Act to the Plaintiffs, American nationals 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.

A. DEUTSCHE BANK'S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY

176. From at least 1999 through 2011, Defendant laundered at least \$10 billion dollars for rogue regimes subject to U.S. sanctions, including Iran, encompassing entities on OFAC's SDN List.

177. Defendant participated in the Conspiracy using three primary methods:

- (i) removing from SWIFT payment messages information that identified an underlying party to the transaction as an entity subject to U.S. sanctions;
- (ii) using nontransparent cover payments, which enabled Defendant to send payment messages to the U.S. that did not include information identifying an underlying party to the transactions as a possibly-sanctioned entity; and
- (iii) including notes or code words, or instructing customers to include notes or code words, in payment messages to ensure Defendant's staff employed special processing to hide any sanctions relationship before sending the payments to the U.S.

178. Defendant's employees recognized that these handling processes were necessary in order to evade the sanctions-related protections and controls of Deutsche Bank New York and other correspondents.

179. For example, a 2003 internal email stated that Deutsche Bank employs "specific precautionary measures that require a great deal of expertise" because "[i]f we make a mistake, the amounts to be paid could be frozen in the USA and/or DB's business interests in the USA could be damaged."

180. Similarly, the Assistant Vice President who oversaw payments processing explained to a colleague who inquired about Iranian payments, Defendant needed to employ "the tricks and cunning of MT103 and MT202" because of the U.S. sanctions restrictions otherwise applicable to sanctions-related payments.

181. Therefore, as explained in another email summing up the process for handling Iran-related payments, Defendant's preferred method was to process a payment using the cover payment method (MT202 transfers), and when that was not possible, "we will arrange for the order to be dropped ... into a further repair queue, where the references to the [Iranian] principal will then be eliminated."

182. On some occasions, payments that were rejected by Deutsche Bank New York due to a suspected sanctions connection were simply resubmitted to a different U.S. correspondent bank by the overseas office.

183. Alternatively, some payments that were rejected in the U.S. when they were sent as MT103 serial payments (which included details about the underlying parties) were then resubmitted as MT202 cover payments – in other words, since the information included on the more detailed message caused the rejection, the overseas office simply sent the payment again using the less transparent method.

184. The special processing that Deutsche Bank used to handle sanctioned payments required manual intervention to identify and process the payments that needed “repair” so as to avoid triggering any sanctions-related suspicions in the U.S.

185. When customers whose payments received this special processing questioned the extra fees Deutsche Bank charged for the manual processing, they were told that processing was required to circumvent the U.S.-based sanctions controls.

186. Bank relationship managers and other employees worked with Defendant’s sanctioned customers to conceal the details about their payments from U.S. correspondent banks.

187. During site visits, in emails, and during phone calls, clients were instructed to include special notes or code words in their payment messages that would trigger special handling by Defendant before the payment was sent to the United States.

188. The Bank’s Iranian co-conspirators often included notes in free-text fields of SWIFT messages such as:

- a. “PLS DON’T MENTION THE NAME OF BANK SADERAT IRAN OR IRAN IN USA”

b. "THE NAME BANK MELLI OR MARKAZI SHOULD NOT BE MENTIONED...IMPORTANT: NO IRANIAN NAMES TO BE MENTIONED WHEN MAKING PAYMENT TO NEW YORK."

189. But Defendant did not rely solely on notes and code words from its Iranian co-conspirators.

190. In fact, Defendant actually marketed its criminal conduct as an "OFAC-safe" handling process and touted its experience in handling sanctions-related payments.

191. Some of Defendant's employees were even considered "experts" in its "OFAC-safe" handling procedures. They regularly educated colleagues in other branches or in other divisions outside the U.S. about handling U.S. dollar payments.

192. In addition, at least one member of Defendant's Management Board was kept apprised, and approved, of Defendant's criminal conduct.

193. Moreover, Defendant prepared a training manual for newly-hired payments staff in an overseas office. The manual included a section titled "US Embargo Payments" that explained how to handle payments with a sanctions connection. An early draft included a warning, in bolded text:

**Special attention has to be given to orders in which countries/institutes with embargos are involved. Banks under embargo of the US (e.g., Iranian banks) must not be displayed in any order to [Deutsche Bank New York] or any other bank with American origin as the danger exists that the amount will be frozen in the USA. [Boldface in the original.]**

194. A revised version of the payments manual admonished that payments from Iran and Syria "have to be treated with caution as [ ] the payment gets released from the queue; there is a probability that the funds will be frozen by the Federal Reserve thereby causing financial and reputation loss for the Bank."



195. A later version of the manual noted that the payment message might include key words such as “Embargo” or “Do not pay via US,” but it also cautioned employees that code words might not necessarily be present.

196. Not only did Defendant’s employees enthusiastically participate in the Conspiracy, but even its compliance department was complicit.

197. For example, one relationship manager who asked for advice about U.S. dollar processing was told, “Please be informed that any info on OFAC-safe business patterns (THAT DB does it and HOW DB does it) is strictly confidential information. Compliance does not want us to distribute such info to third parties, and forbids us explicitly to do so in any written or electronic form.” (Emphasis added.)

198. Although Defendant generally tried to shield its New York branch and U.S. subsidiary from its widespread illegal conduct on behalf of Iran (and other sanctioned countries), Defendant’s New York staff were aware of Defendant’s business relationship with U.S.-sanctioned parties.

199. On November 4, 2015, the New York State Department of Financial Services (“DFS”) announced that Deutsche Bank would pay \$258 million dollars for New York Banking Law violations in connection with transactions on behalf of countries and entities subject to U.S. sanctions, including Iran, Libya, Syria, Burma, and Sudan.

200. Deutsche Bank agreed to pay \$200 million to DFS and \$58 million to the Federal Reserve.

201. In a consent order signed with DFS on November 3, 2015 (attached as Exhibit A to the Complaint), Deutsche Bank acknowledged, *inter alia*, that:

- Bank employees developed and employed several processes to handle dollar payments in nontransparent ways that circumvented the controls designed to detect potentially-problematic payments.
- Bank staff in overseas offices handling Message Type 103 serial payment messages, or MT103s, removed information indicating a connection to a sanctioned entity before the payment was passed along to the correspondent bank in the U.S. With any potentially-problematic information removed (or, as was done in some cases, replaced with innocuous information, such as showing the bank itself as the originator), the payment message did not raise red flags in any filtering systems or trigger any additional scrutiny or blocking that otherwise would have occurred if the true details were included.
- The Bank used MT202 cover payments to conceal the identities of underlying parties to transactions.
- Bank employees recognized that these handling processes were necessary in order to evade the sanctions-related protections and controls of Deutsche Bank New York and other correspondents.
- On some occasions, payments that were rejected by Deutsche Bank New York due to a suspected sanctions connection were simply resubmitted by the Bank to a different U.S. correspondent by the overseas office.
- Some payments that were rejected in the U.S. when they were sent as MT103 serial payments (which included details about the underlying parties) were then resubmitted by Deutsche Bank as MT202 cover payments.
- Bank relationship managers and other employees worked with the Bank's sanctioned customers in the process of concealing the details about their payments from U.S. correspondents.
- The Bank's payments processing staff were instructed to be on the lookout for any payment involving a sanctioned entity and ensure that no name or other information that might arouse sanctions-related suspicions was sent to the U.S. correspondents, even if the customer failed to include a special note to that effect.
- Bank employees in many overseas offices, in different business divisions, and with various levels of seniority were actively involved or knew of the Bank's sanctions evading activities.
- At least one member of the Bank's Management Board was kept apprised about and approved of the Bank's business dealings with customers subject to U.S. sanctions.

- The Bank disseminated formal and informal written instructions emphasizing the need for utmost care to ensure that no sanctions-related information was included in U.S.-bound payment messages and setting out the various methods to use when processing sanctions-related payments.
- Bank payments processing employees prepared a training manual for newly-hired payments staff in an overseas office. The manual included a section titled “US Embargo Payments” that explained how to handle payments with a sanctions connection. An early draft included a warning, in bolded text: “Special attention has to be given to orders in which countries/institutes with embargos are involved. Banks under embargo of the US (e.g., Iranian banks) must not be displayed in any order to [Deutsche Bank New York] or any other bank with American origin as the danger exists that the amount will be frozen in the USA.”

202. Although Defendant claims to have substantially wound down its business with Iran in 2007, before 2007 it had entered into a number of financing arrangements that continued through December 31, 2013, with the National Iranian Oil Company (NIOC) and Bank Melli Iran by which it agreed to continue participating in the Conspiracy.

203. Defendant also helped facilitate numerous transactions on behalf of IRISL and its various alter-egos and fronts<sup>6</sup> between September 2008 and February 2010 after the U.S. Treasury Department’s September 10, 2008 designation of IRISL.

204. These transactions were in U.S. dollars and were routed through Defendant’s U.S. subsidiary, Deutsche Bank Trust Company Americas.

**B. BANK SADERAT’S AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY**

205. 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 (Bank Saderat Plc) and branches in Frankfurt, Paris, Athens, Dubai and Beirut.

206. Bank Saderat Iran was nationalized after the Iranian Revolution, but allegedly

---

<sup>6</sup> IRISL operations have been executed through a network of subsidiaries and agents, including, among others, Asia Marine Network PTE. LTD. (a.k.a. Asian Perfect Marine PTE. LTD., a.k.a. IRISL Asia PTE. LTD.) Oasis Freight Agencies (a.k.a. Oasis Freight Agencies LLC) in the UAE, and Irinvestship LTD. in the UK.

privatized in 2009. Bank Saderat Iran maintains that 49% of its shares are owned by the Iranian Government, but it is technically a non-governmental entity.

207. In 2002, Bank Saderat Iran's London bank branch became a subsidiary, incorporated under United Kingdom law, *i.e.* Bank Saderat Plc.

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

209. On September 8, 2006, OFAC amended § 560.516 of the Iranian Transaction Regulations and excluded Bank Saderat from the U-Turn exemption.

210. In announcing the 2006 change to the ITRs excluding Bank Saderat from the U-Turn exemption, OFAC's announcement 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....

211. 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."

212. 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."

213. 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."

214. For many years preceding the revocation of its U-Turn exemption, Bank Saderat

illegally routed its U.S. dollar transactions through the United States with the assistance of various Western financial institutions, including Defendant.

215. In October 2007, Bank Saderat Iran was designated an SDGT pursuant to E.O. 13224. The U.S. Treasury Department press release announcing 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.

216. Defendant conspired with Bank Saderat by knowingly altering, falsifying, or omitting information from U.S. dollar payment messages on Bank Saderat's behalf, helping fund Iranian-sponsored terrorism through Bank Saderat's role as a "significant facilitator of Hezbollah's financial activities" and "conduit between the Government of Iran and Hezbollah."

217. Bank Saderat provided tens of millions of dollars to Hezbollah, substantially assisting Hezbollah in carrying out its terrorist activities in Iraq, including Hezbollah's role in supplying EFPs and training terror cells how to use EFPs – the very weapons that injured the Plaintiffs.

218. Defendant conspired with Bank Saderat by knowingly altering, falsifying, or omitting information from U.S. dollar payment messages on behalf of Bank Saderat, an Iranian bank engaged in criminal activities on behalf of a State Sponsor of Terrorism, and knew or was deliberately indifferent to, and reasonably foresaw, that Bank Saderat would be able to launder tens of millions of dollars to Hezbollah, and Americans like the Plaintiffs herein would be killed or maimed by Iranian proxies.

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

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

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

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

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

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.

223. Bank Melli Iran was designated an SDN pursuant to E.O. 13382 in October 2007, and included on OFAC's SDN list, which resulted in, *inter alia*, its exclusion from the U-Turn exemption. 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.

224. In addition, in mid-2007, Bank Melli in Hamburg (“BMI Hamburg”) transferred funds for DIO, whose weapons caches seized from the Special Groups in Iraq comprised large quantities of weapons produced by Iran in 2006 and 2007, including many 107 mm artillery rockets as well as rounds and fuses for 60 mm and 81 mm mortars.

225. Defendant conspired with Bank Melli by knowingly altering, falsifying, or omitting information from U.S. dollar payment messages on behalf of Bank Melli, helping Bank Melli send “at least \$100 million to the Qods Force,” which organized and conducted attacks on Coalition Forces, including the Plaintiffs.

226. Bank Melli provided at least \$100 million dollars to the IRGC-QF, substantially assisting Iran in carrying out its terrorist activities in Iraq, including the IRGC-QF’s role in supplying EFPs and training terror cells how to use EFPs – the very weapons that injured the Plaintiffs.

227. Defendant conspired with Bank Melli by knowingly altering, falsifying, or omitting information from U.S. dollar payment messages on behalf of Bank Melli, an Iranian bank engaged in criminal activities on behalf of a State Sponsor of Terrorism, and knew or was deliberately indifferent to, and reasonably foresaw, that Bank Melli would be able to launder \$100 million dollars to the IRGC-QF, and Americans like the Plaintiffs herein would be killed or maimed by Iranian proxies.

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

228. The Central Bank of Iran is fully controlled and run by individuals directly appointed by the Government of Iran.

229. 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 the CBI's purpose limited to "regulating" Iranian banks and managing Iran's currency and internal interest rates.

230. 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 and Bank Saderat as conduits for terror financing and weapons proliferation on behalf of the Iranian regime.

231. At all relevant times, the CBI was an active participant in the Conspiracy. For example, leading up to the adoption of U.N. 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.

232. Throughout the relevant time period, the CBI maintained accounts at Bank Melli and Bank Saderat in various currencies.

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

234. 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.

235. As part of the Conspiracy, the CBI utilized Bank Saderat to transfer funds to Hezbollah.

236. By knowingly altering, falsifying, or omitting information from U.S. dollar payment messages that it facilitated on behalf of the CBI, Defendant participated in the Conspiracy through which the CBI helped fund Iranian-sponsored terrorism through its direct



involvement in facilitating Saderat's role as a "significant facilitator of Hezbollah's financial activities."

237. The CBI provided tens of millions of dollars to Hezbollah, substantially assisting Hezbollah in carrying out its terrorist activities in Iraq, including Hezbollah's role in supplying EFPs and training terror cells how to use EFPs – the very weapons that injured the Plaintiffs.

238. By knowingly altering, falsifying, or omitting information from U.S. dollar payment messages that it facilitated on behalf of the CBI, an Iranian bank engaged in criminal activities on behalf of a State Sponsor of Terrorism, Defendant knew or was deliberately indifferent to, and reasonably foresaw, that the CBI would be able to launder tens of millions of dollars to Hezbollah, and Americans like the Plaintiffs herein would be killed or maimed by Iranian proxies.

#### CLAIMS FOR RELIEF

##### FIRST CLAIM FOR RELIEF

##### CIVIL LIABILITY UNDER 18 U.S.C. § 2333(a) FOR VIOLATIONS OF 18 U.S.C. § 2339A CONSTITUTING ACTS OF INTERNATIONAL TERRORISM

239. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

240. By knowingly agreeing to provide, and providing, material support to Iran in an illegal manner, and knowing, or being deliberately indifferent to the fact, that 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, Defendant violated § 2339A's express prohibition against conspiring to provide material support within the meaning set forth in that provision, and committed and completed overt acts in furtherance of the Conspiracy.

241. Defendant's conduct in agreeing to provide Iran with millions (or more) of U.S. dollars in an illegal manner violated 18 U.S.C. § 2339A's express prohibition against providing material support or resources, or concealing or disguising or attempting or conspiring to conceal or disguise 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).

242. 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.

243. The Conspiracy among Iran and its agents and Defendant and other non-defendant co-conspirators resulted in the transfer of: (a) more than two hundred billion dollars in U.S. currency 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.

244. Defendant together with other non-defendant co-conspirators (including Iran) agreed to, and did in fact, purposefully transfer billions of U.S. dollars through the United States knowing that such funds would be delivered to Iran and Iranian agents, and that the payment messages facilitating such funds transfers had been deliberately and intentionally structured 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.

245. At the time Defendant knowingly agreed to provide Iran material support in an illegal manner, 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 enable it to cultivate and support terrorism.

246. 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 the 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).

247. 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), or acts of international terrorism (18 U.S.C. § 2331), including facilitating, funding, preparing for, and supporting terrorist activity by the Special Groups.

248. Through this clandestine stream of U.S. dollars, Defendant knew, or was deliberately indifferent to the fact, that its participation in the Conspiracy to provide Iran with illegal material support would foreseeably (and in fact did) facilitate 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 Defendant.

249. Defendant knowingly and purposefully agreed to provide 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 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/or the Special Groups (including Kata'ib Hezbollah), 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/or the Special Groups.

250. The material support that Defendant knowingly agreed to illegally provide to Iran, provided reasonably 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, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused the Plaintiffs' injuries.

251. Defendant also knew of the existence of other conspirators; that the other conspirators (including the 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 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.

252. 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 it performed in furtherance of the Conspiracy facilitated that specific objective.

253. 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 constrain Iran's sponsorship of terrorism and terrorist organizations (including Weapons of Mass Destruction proliferation activities in furtherance of such sponsorship), 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).

254. Defendant's overt acts and agreement to purposefully transfer millions 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.

255. Defendant's agreement to enter into the Conspiracy and purposefully transfer 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/or the Special Groups, and its acts in furtherance of the Conspiracy were therefore acts of international terrorism because they either were, or objectively appear 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/or the Special Groups' abilities to prepare for, support, fund, train, initiate, and/or carry out mass destruction and murder.

256. 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, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f and 2339A). Defendant's conduct was thus also a substantial, reasonably foreseeable factor in bringing about the Plaintiffs' injuries.

257. Furthermore, each Plaintiff's injuries constitutes a harm falling within the reasonably foreseeable risk contemplated by Defendant's violations, including Defendant's knowing agreement to enter into the Conspiracy, Defendant's performance of overt acts in furtherance of the Conspiracy, and 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, Bank Saderat, and the IRISL) enacted specifically to ensure that Iran had restricted access to U.S. dollars and financial services under conditions of maximum transparency, that such dollars were not to be used by or for the benefit of SDNs, that such U.S. dollars would not facilitate Iran's efforts to acquire, develop, and distribute Weapons

of Mass Destruction (including weapons such as EFPs directed at Coalition Forces) and that any funds Iran did receive that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies.

258. 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, 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) FOR VIOLATIONS OF 18 U.S.C. §**  
**2339B CONSTITUTING ACTS OF INTERNATIONAL TERRORISM**

259. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

260. By knowingly agreeing to provide, and providing, material support to Iran in an illegal manner, and knowing, or being deliberately indifferent to the fact, that the objects and aims of the Conspiracy were to provide material support to Foreign Terrorist Organizations, Defendant violated § 2339B's express prohibition against conspiring to provide material support within the meaning set forth in that provision, and committed and completed overt acts in furtherance of the Conspiracy.

261. Defendant and Iran agreed to, and did in fact, purposefully transfer millions of dollars through the United States expressly in a manner designed to purposefully 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 tens of millions of dollars in payments to Hezbollah through the international financial system. In doing so, Defendant was willing to, and did, commit 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, which provided material support to FTOs that were responsible for Plaintiffs' injuries.

262. At the time Defendant knowingly agreed to provide Iran material support in an illegal manner, Defendant knew that Iran had been officially designated by the United States as a State Sponsor of Terrorism since 1984, subject to various U.S. sanctions, and knew or was deliberately indifferent to the fact 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.

263. As a result of its extensive U.S. operations, Defendant knew, or was deliberately indifferent to the fact, that Hezbollah was designated an FTO at all times relevant to this action. Defendant also knew that Hezbollah engaged in terrorist activities (8 U.S.C. § 1183(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331).

264. Defendant knew or was deliberately indifferent to the fact that its agreement to provide Iran material support in an illegal manner, and the overt acts it completed in connection with the Conspiracy, unlawfully evaded U.S. sanctions and regulations directed at mitigating the risk that Iran would carry out, support, fund, plan for, prepare, conspire with, or facilitate acts of international terrorism by FTOs, including acts planned, attempted, and perpetrated by Iran's proxy, agent, and strategic partner, Hezbollah.

265. 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.



266. Defendant also knew of the existence of other conspirators; that the other conspirators (including the Iranian Bank Co-conspirators) engaged in the same or similar conduct; and that the other conspirators shared the objective of providing material support and services to Iran 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.

267. 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 it performed in furtherance of the Conspiracy facilitated that specific objective.

268. 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), Defendant also knew, or was deliberately indifferent to the fact, that the Conspiracy's aims would foreseeably result in Iran transferring millions of dollars to Hezbollah, an FTO.

269. The material support that 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, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f, and that have caused injuries to the Plaintiffs.

270. Defendant's overt acts in entering into the Conspiracy and knowingly agreeing to provide Iran – a known and designated State Sponsor of Terrorism – material support and services in an illegal manner, and resultant, purposeful transfer of millions of U.S. dollars 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.

271. Defendant's agreement to enter into the Conspiracy and purposeful transfer of millions 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 either were, or objectively appear 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 and injuring hundreds of American nationals in Iraq.

272. 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/or commit acts of international terrorism under the definition set forth in 18 U.S.C. § 2331. Defendant's conduct was thus also a substantial, foreseeable factor in bringing about the Plaintiffs' injuries.

273. Furthermore, each Plaintiff's injuries constitutes a harm falling within the risk contemplated by Defendant's violations, including Defendant's knowing agreement to enter into the Conspiracy, the overt acts Defendant performed in furtherance of the Conspiracy, and Defendant's knowledge of, or deliberate indifference to, the fact that a specific, reasonably 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.

274. 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, 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).

**PRAYER FOR RELIEF**

WHEREFORE, the Plaintiffs pray that this Court:

- (a) Accept jurisdiction over this action;
- (b) Enter judgment against Defendant and in favor of the Plaintiffs for compensatory damages in amounts to be determined at trial;
- (c) Enter judgment against Defendant and in favor of the Plaintiffs for treble damages pursuant to 18 U.S.C. § 2333(a);
- (d) Enter judgment against Defendant and in favor of the 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 Defendant has 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: May 4, 2016

**OSEN LLC**  
**Lead Counsel (Local Rule 5.1(a))**

By /s/ Gary M. Osen  
Gary M. Osen (NJ Bar No. 030731993)  
Ari Ungar  
Aaron Schlanger  
Naomi B. Weinberg  
Peter Raven-Hansen, Of Counsel  
2 University Plaza, Suite 201  
Hackensack, NJ 07601  
(201) 265-6400  
(201) 265-0303 Fax

**DOWD & DOWD, P.C.**

By /s/ Douglas P. Dowd  
Douglas P. Dowd (#29240MO)  
211 North Broadway, Suite 4050  
St Louis, MO 63102  
(314) 621-2500  
(314) 621-2503 Fax

**TURNER & ASSOCIATES, P.A.**  
Tab Turner  
4705 Somers Avenue, Suite 100  
North Little Rock, AR 72116  
(501) 791-2277

Attorneys for Plaintiffs

NEW YORK STATE DEPARTMENT  
OF FINANCIAL SERVICES

In the Matter of

DEUTSCHE BANK AG,  
DEUTSCHE BANK AG NEW YORK BRANCH

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

The New York State Department of Financial Services (the “Department”), Deutsche Bank AG (“Deutsche Bank” or the “Bank”), and Deutsche Bank AG New York Branch (“New York Branch”) stipulate that:

WHEREAS Deutsche Bank is a major international banking institution with more than 98,000 employees and total assets exceeding \$1.9 trillion;

WHEREAS Deutsche Bank operates a foreign bank branch in New York State that is licensed, supervised, and regulated by the Department;

WHEREAS Deutsche Bank Trust Company Americas (“DBTCA”), a subsidiary of Deutsche Bank AG, is chartered pursuant to Article III of the New York Banking Law and subject to supervision and regulation by the Department;

WHEREAS during the relevant time period, both the New York Branch and DBTCA (collectively, “Deutsche Bank New York”) conducted correspondent banking and U.S. dollar clearing activities, as explained more fully below;

WHEREAS from at least 1999 through 2006, Deutsche Bank used non-transparent methods and practices to conduct more than 27,200 U.S. dollar clearing transactions<sup>1</sup> valued at over \$10.86 billion on behalf of Iranian, Libyan, Syrian, Burmese, and Sudanese financial institutions and other entities subject to U.S. economic sanctions, including entities on the Specially Designated Nationals (“SDN”) List of the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”);<sup>2</sup>

WHEREAS the Bank effectively concealed the relationship of a sanctioned or possibly-sanctioned party to the transactions by knowingly processing these non-transparent transactions using methods such as (i) removing from SWIFT payment messages<sup>3</sup> information that identified an underlying party to the transaction as an entity subject to U.S. sanctions; (ii) using non-transparent cover payments, which enabled the bank to send payment messages to the U.S. that did not include information identifying an underlying party to the transactions as a possibly-sanctioned entity; and (iii) including notes or code words, or instructing customers to include notes or code words, in payment messages to ensure bank staff employed special processing to hide any sanctions relationship before sending the payments to the U.S.;

WHEREAS by knowingly processing transactions involving sanctioned entities using non-transparent methods, Deutsche Bank failed to maintain accurate records as to those transactions, subverted Deutsche Bank New York’s and correspondent banks’ controls designed

---

<sup>1</sup> U.S. dollar clearing is the process by which U.S. dollar-denominated payments between counterparties are made through a bank in the United States.

<sup>2</sup> Deutsche Bank reported, employing extrapolation methodology to the transaction messages reviewed, that over 600 of those transactions valued at more than \$38 million were illegal under various U.S. Sanctions and other programs.

<sup>3</sup> The Society of Worldwide Interbank Financial Telecommunications, or SWIFT, provides an international network through which banks exchange electronic wire transfer messages. SWIFT messages contain various informational fields.

to detect possibly illegal transactions, and prevented effective review by regulators and other authorities;

WHEREAS Deutsche Bank's conduct ran counter to U.S. foreign policy and national security interests, constituted violations of New York and federal laws and regulations, and raises substantial safety and soundness concerns;

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Sections 39 and 44 of the Banking Law, the Department and Deutsche Bank agree to the following:

#### **Factual Background**

##### Use of Wire Stripping and Non-Transparent Cover Payments to Disguise Transactions

1. Starting at least in 1999, Bank employees recognized that U.S. sanctions rules, which applied at that time or over the course of subsequent years to Iranian, Syrian, Libyan, Burmese, or Sudanese customers or to customers who were listed on OFAC's SDN list, would pose problems for U.S. dollar payments sent to or cleared through the U.S., including clearing done through Deutsche Bank New York. Payments involving sanctioned entities were subject to additional scrutiny and might be delayed, rejected, or frozen in the United States. In order to facilitate what it saw as "lucrative" U.S. dollar business for sanctioned customers, Bank employees developed and employed several processes to handle dollar payments in non-transparent ways that circumvented the controls designed to detect potentially-problematic payments.

2. One method was wire stripping, or alteration of the information included on the payment message. Bank staff in overseas offices handling Message Type 103 serial payment messages, or MT103s, removed information indicating a connection to a sanctioned entity before

the payment was passed along to the correspondent bank in the U.S.<sup>4</sup> With any potentially-problematic information removed (or, as was done in some cases, replaced with innocuous information, such as showing the bank itself as the originator), the payment message did not raise red flags in any filtering systems or trigger any additional scrutiny or blocking that otherwise would have occurred if the true details were included.

3. A second method was the use of non-transparent cover payments. The cover payment method involved splitting an incoming MT103 message into two message streams: an MT103, which included all details, sent directly to the beneficiary's bank, and a second message, an MT202, which did not include details about the underlying parties to the transaction, sent to Deutsche Bank New York or another correspondent clearing bank in the U.S. In this way, no details that would have suggested a sanctions connection and triggered additional delay, blocking, or freezing of the transactions were included in the payment message sent to the U.S. bank.

4. Bank employees recognized that these handling processes were necessary in order to evade the sanctions-related protections and controls of Deutsche Bank New York and other correspondents. For example, a relationship manager who handled significant business for Iranian, Libyan, and Syrian customers explained the need for special measures as follows, in a 2003 email to colleagues: The Bank employs "specific precautionary measures that require a great deal of expertise" because "[i]f we make a mistake, the amounts to be paid could be frozen in the USA and/or DB's business interests in the USA could be damaged." Or as the Assistant Vice President who oversaw payments processing explained to a colleague who inquired about

---

<sup>4</sup> A serial payment consisted of a SWIFT MT103 sent from the ordering customer's bank through a correspondent bank and on to the beneficiary's bank.



Iranian payments, the Bank needed to employ “the tricks and cunning of MT103 and MT202” because of the U.S. sanctions restrictions otherwise applicable to sanctions-related payments.

5. Therefore, as explained in another email summing up the process for handling Iran-related payments, the Bank’s preferred method was to process a payment using the cover payment method, and when that was not possible, “we will arrange for the order to be dropped . . . into a further repair queue, where the references to the principal will then be eliminated.”

6. As new sanctioned customers were brought into the fold, or as newly-enacted U.S. sanctions programs affected existing customers, these processes were extended so as to ensure that payments did not encounter U.S.-based sanctions problems. For example, when Bank staff learned that possible new U.S. sanctions might affect certain Syrian customers, they discussed how Syrian payment orders “must be ‘anonymised’ in the same way as orders from Iran or Libya, i.e. coverage without mention of Syria can be directed via USA and the order is made directly to the beneficiary’s bank.”

7. On some occasions, payments that were rejected by Deutsche Bank New York due to a suspected sanctions connection were simply resubmitted to a different U.S. correspondent by the overseas office. Alternatively, some payments that were rejected in the U.S. when they were sent as MT103 serial payments (which included details about the underlying parties) were then resubmitted as MT202 cover payments – in other words, since the information included on the more detailed message caused the rejection, the overseas office simply sent the payment again using the less transparent method.

8. The special processing that the Bank used to handle sanctioned payments was anything but business as usual; it required manual intervention to identify and process the

payments that needed “repair” so as to avoid triggering any sanctions-related suspicions in the U.S. Indeed, on occasion, customers whose payments received this special processing questioned the extra fees the bank was charging for the manual processing. They were told that this is what was necessary in order to circumvent the U.S.-based sanctions controls.

9. The Bank instituted a series of policies starting in 2006 to end these practices and wind down business with U.S.-sanctioned entities. However, some instances of resubmitting rejected payments or processing sanctions-related payments through New York persisted even after the formal policies were instituted.

Bank Staff Coordinated With Sanctioned Customers to Conceal True Details About Payments

10. Bank relationship managers and other employees worked with the Bank’s sanctioned customers in the process of concealing the details about their payments from U.S. correspondents.

11. During site visits, in emails, and during phone calls, clients were instructed to include special notes or code words in their payment messages that would trigger special handling by the bank before the payment was sent to the United States. Sanctioned customers were told “it is essential for you to continue to include [the note] ‘Do not mention our bank’s name...’ in MT103 payments that may involve the USA. [That note] ensures that the payments are reviewed prior to sending. Otherwise it is possible that the [payment] instruction would be sent immediately to the USA with your full details. . . . [This process] is a direct result of the US sanctions.” Customers, in turn, included notes in free-text fields of SWIFT messages such as “Please do not mention our bank’s name or SWIFT code in any msg sent via USA,” “PLS DON’T MENTION THE NAME OF BANK SADERAT IRAN OR IRAN IN USA,” or “THE NAME BANK MELLI OR MARKAZI SHOULD NOT BE MENTIONED . . . IMPORTANT:

NO IRANIAN NAMES TO BE MENTIONED WHEN MAKING PAYMENT TO NEW YORK.”

12. But the Bank did not rely on the customer notes and code words alone; the Bank’s payments processing staff were instructed to be on the lookout for any payment involving a sanctioned entity and ensure that no name or other information that might arouse sanctions-related suspicions was sent to the U.S. correspondents, even if the customer failed to include a special note to that effect.

13. In fact, the Bank’s “OFAC-safe” handling processes and its experience in handling sanctions-related payments were selling points when soliciting new business from customers subject to U.S. sanctions. On one occasion, a relationship manager visiting a Syrian bank during a time when the U.S. was considering instituting certain Syrian sanctions pitched Deutsche Bank’s “OFAC-safe vehicles,” and when the client mentioned possibly splitting its business among several Asia-based banks, the relationship manager “highlighted that the Asian banks in general are not very familiar with OFAC procedures [and] [a]sked them to consider who their friends will be in the longer run, DB or Asian banks.” In another instance, after Deutsche Bank staff responded to a client inquiry about handling U.S. dollar payments relating to Iran and Syria with a favorable “OFAC safe” solution, the Bank relationship manager reported that the client was so pleased that it “used the opportunity to enquire whether we can also do USD payments into Burma/Myanmar.”

Deutsche Bank’s Practice Was Widespread and Formalized, But Care Was Taken Not to Make Too Much “Noise” About the Practice or the Business the Bank Was Handling

14. The practice of non-transparent payment processing was not isolated or limited to a specific relationship manager or small group of staff. Rather, Bank employees in many

overseas offices, in different business divisions, and with various levels of seniority were actively involved or knew about it.

15. In addition, some evidence indicates that at least one member of the Bank's Management Board was kept apprised about and approved of the Bank's business dealings with customers subject to U.S. sanctions.

16. Certain non-U.S. employees, especially those who managed relationships with a high number of Iranian, Libyan, or Syrian clients or who regularly processed U.S. dollar payments for sanctioned customers, were considered experts in the bank's "OFAC-safe" handling procedures. They regularly educated colleagues in other branches or in other divisions outside the U.S. about handling U.S. dollar payments.

17. Moreover, the Bank disseminated formal and informal written instructions emphasizing the need for utmost care to ensure that no sanctions-related information was included in U.S.-bound payment messages and setting out the various methods to use when processing sanctions-related payments.

18. For example, Deutsche Bank staff told investigators that during the earlier part of the relevant time period, an internal customer database included notes for certain sanctioned customers indicating that their name must not be referenced in payment messages sent to the U.S.

19. Later, Bank payments processing employees prepared a training manual for newly-hired payments staff in an overseas office. The manual included a section titled "US Embargo Payments" that explained how to handle payments with a sanctions connection. An early draft included a warning, in bolded text: "Special attention has to be given to orders in which countries/institutes with embargos are involved. Banks under embargo of the US (e.g.,

Iranian banks) must not be displayed in any order to [Deutsche Bank New York] or any other bank with American origin as the danger exists that the amount will be frozen in the USA.”

20. A revised version of the payments manual admonished that payments from Iran and Syria “have to be treated with caution as [ ] the payment gets released from the queue; there is a probability that the funds will be frozen by the Federal Reserve thereby causing financial and reputation loss for the Bank.” A later version of the manual noted that the payment message might include key words such as “Embargo” or “Do not pay via US,” but it also cautioned employees that code words might not necessarily be present. In any event, non-U.S. employees were instructed that information linking a customer to a U.S. sanctions program must not be displayed in any message sent to Deutsche Bank New York or any other American bank. The preference, they were told, was to send two messages (that is, to use the cover payment method), but if that was not possible, they must reformat the message so that it gets routed for additional repair and reformatting “in such a way that the Embargo names are not visible to the receiving US banks.” The manual included computer screenshots illustrating how these problematic messages might appear and how to handle them.

21. Moreover, less formal instructions were disseminated to certain staff via email throughout the relevant time period. In one email chain regarding possible recruitment of a new customer with Libyan connections, Bank staff were cautioned to “please be careful in regard to the US, since it does violate OFAC,” and were told, “please do not mention OFAC names in the subject line of e-mails!” In another instance, when certain U.S. regulations against a Syrian bank were imposed in 2004, relevant employees were told: “Let us be very careful while effecting USD denominated transaction[s] with Syria. In case we have to effect any USD denominated remittance to Syria, please ensure that name of Syria should not appear in the message.”

22. At the same time, Bank staff took care to avoid publicizing details about their non-transparent payments handling, both within and outside the bank. Employees recognized the legal and reputational concerns and acted to keep the payment handling methods – and indeed the fact of the bank’s business dealings with sanctioned entities in general – on a need-to-know basis.

23. For example, one non-U.S. relationship manager who asked for advice about U.S. dollar processing was told, “Please be informed that any info on OFAC-safe business patterns (THAT DB does it and HOW DB does it) is strictly confidential information. Compliance does not want us to distribute such info to third parties, and forbids us explicitly to do so in any written or electronic form.” In another email, a senior compliance executive with oversight of this area told a non-U.S. relationship manager who was asking about the possibility of doing business with a Syrian customer that Compliance “agreed to do business on a low key level without public announcements etc.” Later, when that relationship manager was offering advice to another non-U.S. colleague about assisting a client who needed to make and receive U.S. dollar payments with Iranian and Syrian connections, he cautioned his colleague: “As usual, let’s not revert to the client in writing due to the reputational risk involved if the e-mail goes to wrong places. Someone should call [the client] and tell them orally and ensure that the conversation is not taped. . . . Let’s also keep this e-mail strictly on a ‘need-know’ basis, no need to spread the news in [Deutsche Bank’s Asian offices about] what we do under OFAC scenarios.”

24. Around the same time, that same relationship manager told another non-U.S. colleague: “Please note that while DB is prepared to do business with Syria, we obviously have sizeable business interests in the US, too, which DB wants to protect. So any Syrian transaction should be treated STRICTLY confidential and should involve any colleagues on a ‘Must-Know’

basis only! . . . [W]e do not want to create any publicity or other ‘noise’ in the markets or media.”

25. In addition, while one of the main purposes of the nontransparent practices was to keep the Bank’s U.S. staff in the dark about the sanctions connections of the payments they were processing, Deutsche Bank New York staff occasionally raised objections to the Bank’s business relationship with U.S.-sanctioned parties based on U.S. law. Their European colleagues, however, did nothing to stop the practice but instead redoubled their efforts to hide the details from their American colleagues. For example, a relationship manager who did significant business with Iranian and Syrian customers complained to his boss that colleagues in the Middle East “participated in a major conference call with senior management of [Deutsche Bank New York] and provided an overview of DB’s account activities with Syria outside the U.S. Senior management of [Deutsche Bank New York] complained strongly to DB Frankfurt that they see this as a breach of law.” The relationship manager viewed this incident not as a prompt to re-examine the bank’s Syrian business, however, but rather as indicating a need to better train the non-U.S. staff who handle the “very lucrative” Syrian and Iranian business to ensure such disclosures do not occur in the future.

#### **Violations of Law and Regulations**

26. Deutsche Bank failed to maintain or make available at Deutsche Bank New York true and accurate books, accounts, and records reflecting all transactions and actions, in violation of New York Banking Law §§ 104 and 200-c.

27. Deutsche Bank employees knowingly made and caused to be made false entries in the Bank’s books, reports, and statements and omitted and caused to be omitted therefrom true entries of material particular pertaining to the U.S. dollar clearing business of the Bank at

Deutsche Bank New York, with the intent to deceive the Superintendent and examiners of the Department and representatives of other U.S. regulatory agencies that were lawfully appointed to examine the Bank's condition and affairs, in violation of 3 NYCRR § 3.1.

28. Deutsche Bank failed to submit a report to the Superintendent immediately upon discovering fraud, dishonesty, making of false entries and omission of true entries, or other misconduct, whether or not a criminal offense, in violation of 3 NYCRR § 300.1.

### **Settlement Provisions**

#### **Monetary Payment:**

29. Deutsche Bank shall pay a civil monetary penalty pursuant to Banking Law § 44 to the Department in the amount of \$200,000,000. The Bank shall pay the entire amount within ten days of executing this Consent Order. Deutsche Bank agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

#### **Independent Monitor**

30. The Bank<sup>5</sup> and the Department agree to retain an independent monitor for one year to conduct a comprehensive review of the Bank's existing BSA/AML and OFAC sanctions compliance programs, policies, and procedures in place at the Bank that pertain to or affect activities conducted by or through Deutsche Bank New York.

31. The monitor will be selected by the Department in the exercise of its sole discretion, and will report directly to the Department.

---

<sup>5</sup> For purposes of Paragraphs 30-40, "the Bank" shall mean Deutsche Bank AG, Deutsche Bank AG New York Branch, and DBTCA.



32. Among other things, the monitor will review and report on:
  - a. The elements of the Bank's corporate governance that contributed to or facilitated the improper conduct discussed in this Consent Order and that permitted it to go on, relevant changes or reforms to its corporate governance that the Bank has made since the time of the conduct discussed in this Consent Order, and whether those changes or reforms are likely to significantly enhance the Bank's BSA/AML and OFAC compliance going forward;
  - b. The thoroughness and comprehensiveness of the Bank's current global BSA/AML and OFAC compliance program;
  - c. The organizational structure, management oversight, and reporting lines that are relevant to BSA/AML and OFAC compliance, and an assessment of the staffing of the BSA/AML and OFAC compliance teams, including the duties, responsibilities, authority, and competence of officers or employees responsible for the Bank's compliance with laws and regulations pertaining to BSA/AML or OFAC compliance;
  - d. The propriety, reasonableness, and adequacy of any proposed, planned, or recently-instituted changes to the Bank's BSA/AML and OFAC compliance programs;
  - e. Any corrective measures necessary to address identified weaknesses or deficiencies in the Bank's corporate governance or its global BSA/AML and OFAC compliance program.
33. The Bank agrees that it will fully cooperate with the monitor and support its work by, among other things, providing the monitor with access to all relevant personnel, consultants

and third-party service providers, files, reports, or records, whether located in New York, Germany, or elsewhere, consistent with applicable law.

34. Within forty-five days of receiving the monitor's preliminary written report on its findings, the Bank will submit to the Department a written plan to improve and enhance the current global BSA/AML and OFAC compliance program that pertains to or affects activities conducted by or through Deutsche Bank New York, incorporating any relevant corrective measures identified in the monitor's report (the "Action Plan").

35. The Action Plan will, if required, provide recommendations for enhanced internal controls and updates or revisions to current policies, procedures, and processes in order to ensure full compliance with all applicable provisions of the BSA and related rules and regulations, OFAC requirements and regulations, and the provisions of this Consent Order. If so provided by the monitor, and upon written consent of the Department, the Bank will commence implementation of the monitor's recommendations.

36. Within forty-five days of receiving the monitor's preliminary written report of findings, the Bank will submit to the Department a written plan to improve and enhance management oversight of BSA/AML and OFAC compliance programs, policies, and procedures now in place at the Bank that pertain to or affect activities conducted by or through Deutsche Bank New York, incorporating any relevant corrective measures identified in the monitor's report (the "Management Oversight Plan").

37. The Management Oversight Plan will address relevant matters identified in the monitor's written report of findings and provide a sustainable management oversight framework. Upon written consent from the Department, the Bank will commence implementation of the changes.

38. The monitor will thereafter oversee the implementation of any corrective measures undertaken pursuant to the Action Plan and Management Oversight Plan.

39. Finally, the monitor will assess the Bank's compliance with its corrective measures and will submit subsequent progress reports and a final report to the Department and the Bank, at intervals to be determined by the Department. The Department may, in its sole discretion, extend any reporting deadline set forth in this section.

40. The term of the monitor's engagement will extend for one year from the date of the formal engagement. Any dispute as to the scope of the monitor's authority or mandate will be resolved by the Department in the exercise of its sole discretion, after appropriate consultation with the Bank and the monitor.

#### **Termination of Employees:**

41. While several of the Bank employees who were centrally involved in the improper conduct discussed in this Consent Order no longer work at the Bank, several such employees do remain employed by the Bank.

42. The Department orders Deutsche Bank to take all steps necessary to terminate the following employees, who played central roles in the improper conduct discussed in this Consent Order: a managing director in Global Transactions Banking who was assigned the code number 24; a managing director in Operations who was assigned the code number 325; a director in Operations who was assigned the code number 7; a director in Corporate Banking and Securities who was assigned the code number 11; a vice president in Global Transactions Banking who was assigned the code number 1; and a vice president and relationship manager who was assigned the code number 30. If, after Deutsche Bank has taken whatever action is necessary to terminate these employees, a judicial or regulatory determination or order is issued finding that such action

is not possible under German law, then Deutsche Bank shall ensure, consistent with applicable law, that these employees are not allowed to hold or assume any duties, responsibilities, or activities involving compliance, U.S. dollar payments, or any matter relating to U.S. operations.

43. With respect to the employees who were assigned code numbers 26, 28, and 32, Deutsche Bank shall ensure, consistent with applicable law, that these employees are not allowed to hold or assume any duties, responsibilities, or activities involving compliance, U.S. dollar payments, or any matter relating to U.S. operations.

44. The Department also orders Deutsche Bank to refrain from ever rehiring for any full-time, part-time, or consulting position the following employees, who played central roles in the conduct discussed in this Consent Order but who previously left the Bank: the employees who were assigned the code numbers 15, 20, 29, 34, 35, 37, 71, 75, 80, and 124.

**Breach of Consent Order:**

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

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

**Waiver of Rights:**

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

**Parties Bound by the Consent Order:**

48. This Consent Order is binding on the Department and Deutsche Bank, as well as any successors and assigns that are under the Department's supervisory authority. But this Consent Order does not bind any federal or other state agency or any law enforcement authority.

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

50. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against Deutsche Bank for transactions or conduct that the Bank did not disclose to the Department in the written materials the Bank submitted to the Department in connection with this matter.

**Notices:**

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

For the Department:

James Caputo  
Jared Elostá  
New York State Department of Financial Services  
One State Street  
New York, NY 10004

For Deutsche Bank:

Christof von Dryander  
Deputy General Counsel  
Deutsche Bank AG  
Taunusanlage 12  
60325 Frankfurt Am Main, Germany

Alan Vinegrad  
Covington & Burling LLP  
620 Eighth Avenue  
New York, NY 10018

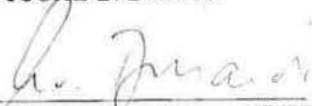
**Miscellaneous:**


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

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

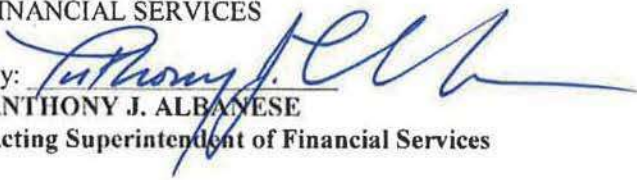
IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed this third day of November, 2015.

DEUTSCHE BANK AG


By:   
CHRISTOF VON DRYANDER  
Deputy General Counsel

By:   
MATHIAS OTTO  
Deputy General Counsel

NEW YORK STATE DEPARTMENT OF  
FINANCIAL SERVICES

By:   
ANTHONY J. ALBANESE  
Acting Superintendent of Financial Services

DEUTSCHE BANK AG NEW YORK BRANCH

By:   
STEVEN REICH  
General Counsel – Americas

By:   
DAVID LEVINE  
Managing Director, Legal

**CERTIFICATE OF SERVICE & CM/ECF FILING**

I hereby certify that on the 21st day of March, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and will be served by the CM/ECF system.

Dated: March 21, 2018

New York, New York

/s/ Peter Raven-Hansen

Peter Raven-Hansen