TORRES LAW

INTERNATIONAL TRADE & NATIONAL SECURITY

Noteworthy OFAC Sanctions Enforcement Actions in 2021

January 2022 | Torres Law, PLLC

***

Torres Law, PLLC is an international trade and national security law firm that assists clients with the import and export of goods, technology, and services. The firm has extensive experience with the various regimes and agencies governing trade such as the Directorate of Defense Trade Controls, the Bureau of Industry and Security, the Office of Foreign Assets Control, the U.S. Customs and Border Protection, and others. Our group provides clients with full support for all trade law issues, including U.S. export control and sanctions laws, industrial security, the Foreign Corrupt Practices Act, anti-boycott laws, and customs laws.

ABOUT TORRES LAW

Torres Law is an international trade and national security law firm that assists clients with the import and export of goods, technology, and services. We have extensive experience with the various regimes and agencies governing national security and trade such as U.S. Customs and Border Protection, the Department of Commerce Bureau of Industry and Security, the Department of State Directorate of Defense Trade Controls, the Department of Treasury Office of Foreign Assets Control, the Committee on Foreign Investment in the United States, the Defense Counterintelligence and Security Agency and others. Our group provides clients with full support for all trade and national security law issues, including U.S. export control and economic sanctions laws, industrial security, and trade strategy and policy.

Global Law Experts 2021 Annual Awards Winner

Ranked in Chambers USA 2021 – Olga Torres

Rated by Super Lawyers

Proud Member of AlliottGlobalAlliance

International Lawyers Network

PRACTICE AREAS

CUSTOMS
U.S. Customs and Border Protection, Border Compliance and EU Customs

EXPORTS
International Traffic in Arms Regulations, Export Administration Regulations, Foreign Trade Regulations Census, and EU Export Controls

ECONOMIC SANCTIONS
Office of Foreign Assets Control (OFAC) and EU Embargoes

FCPA
US and foreign country anti-corruption laws

INDUSTRIAL SECURITY
Committee on foreign investment the US (CFIUS) and Foreign Ownership, Control, or Influence (FOCI)

www.torrestradelaw.com

CONTACT US BY EMAIL AT
info@torrestradelaw.com

TORRES LAW
INTERNATIONAL TRADE & NATIONAL SECURITY

Noteworthy OFAC Sanctions Enforcement Actions in 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") entered into settlement agreements with seventeen companies for violations of various OFAC regulations,[1] issuing civil monetary penalties ranging from $34,329 to $8,572,500, and in one case, issuing a Finding of Violation ("FOV") in lieu of a civil monetary penalty.[2] These enforcement actions offer valuable insight as to the scale and scope of civil penalties imposed by OFAC and underscore the importance of disciplined compliance programs for all companies subject to OFAC regulations.

OFAC imposes civil monetary penalties for violations pursuant to five statutes: the Trading with the Enemy Act ("TWEA"), the International Emergency Economic Powers Act ("IEEPA"), the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA"), the Foreign Narcotics Kingpin Designation Act ("FNKDA"), and the Clean Diamond Trade Act ("CDTA").

***

Cameron International Corporation

On September 27, 2021, OFAC announced a $1,423,766 settlement with Cameron International Corporation ("Cameron"), a Houston, Texas-based supplier of oil and gas goods and services, and a subsidiary of Schlumberger Limited ("Schlumberger") of Curacao, Netherlands, to settle its potential civil liability for apparent violations related to its provision of services to the Russian energy firm Gazprom-Neft Shelf for an offshore oil project. Cameron provided these services when senior managers at Cameron, all U.S. persons, approved five contracts for its foreign subsidiary, Cameron Romania S.R.L. ("Cameron Romania") to supply goods to Gazprom-Neft Shelf's offshore oil platform located in the Russian Arctic. OFAC determined that Cameron's conduct was non-egregious and not voluntarily self-disclosed.

Between July 29, 2015, and November 28, 2016, Cameron violated Directive 4[3] issued pursuant to Executive Order 13662 of March 24, 2014,[4] as implemented pursuant to § 589.201 of the Ukraine-Related Sanctions Regulations. Beginning in July 2015, personnel at Cameron Romania emailed U.S.-person senior managers requesting approvals of Cameron Romania contracts with Gazprom-Neft Shelf. These requests, which were subsequently approved, referenced the

[1] There was an additional OFAC settlement published on December 23 against TD Bank, NA which is not detailed in this digest.
[2] On November 9, 2021, OFAC issued a FOV to Mashreqbank psc for violations of the now-repealed Sudanese Sanctions Regulations, 31 C.F.R. Part 538. OFAC determined the appropriate administrative action was a FOV in lieu of a civil monetary penalty in part because Mashreqbank psc had voluntarily entered into a retroactive statute of limitations waiver agreement, without which OFAC would have been time-barred from charging the violations.
[3] Directive 4, issued September 12, 2014, prohibits U.S. persons within the United States from engaging in the provision, exportation, or re-exportation, directly or indirectly, of goods, services (other than financial services), or technology in support of exploration or production for Deepwater, Arctic offshore, or shale projects that may potentially produce oil in Russia, or in maritime area claimed by Russia and extending from its territory, and that involve any person determined to be subject to this Directive, its property, or its interests in property.
[4] Blocking Property of Additional Persons Contributing to the Situation in Ukraine, Exec. Order No. 13,662, 79 Fed. Reg. 16,167 (Mar. 24, 2014).

provision of oil production or exploration goods to Gazprom-Neft Shelf's Prirazlomnaya platform and stated that the Russian Arctic was the destination of the oil-related goods.

During the relevant time period, Cameron had in place procedures to review prospective transactions with Russian firms to prevent violations of U.S. sanctions. Under these procedures, Cameron personnel were required to complete a form for all transactions involving Russia at the quotation, purchase order, sales order, and delivery stages to collect information for its compliance office to determine Cameron's legal obligations. However, the form did not indicate that U.S.-person involvement in the activities of Cameron's foreign subsidiaries could have fallen within the applicable prohibitions.

On April 1, 2016, Schlumberger acquired Cameron. In connection with its post-acquisition compliance review, Schlumberger discovered the Apparent Violations of Directive 4. In June 2017, Cameron submitted a notification of an apparent violation to OFAC, followed by the submission of an additional report in December 2017. However, OFAC assessed that Cameron's submission did not constitute a voluntary self-disclosure.

Aggravating Factors

(1) U.S.-person senior managers at Cameron were aware that their approvals were for contracts to supply goods to Gazprom-Neft Shelf for Arctic offshore oil production or exploration in the Russian Federation;

(2) Cameron provided real economic benefit to Gazprom-Neft Shelf and acted directly contrary to U.S. foreign policy objectives by approving sales to an entity subject to the restrictions of Directive 4, which is intended to impede Russia's ability to develop frontier or unconventional oil resources; and

(3) Cameron is a large and commercially sophisticated firm with an extensive global presence, operates in an industry and in locations with significant sanctions risk exposure, and was aware of such risks. Therefore, Cameron should have recognized the risk involved in U.S.-person senior managers' approval of a foreign subsidiary's contracts with an entity subject to Directive 4 restrictions.

Mitigating Factors

(1) Cameron and its parent company, Schlumberger, represent that they took meaningful corrective actions upon discovering the apparent violations, including:

a. Identifying all employees who should recuse themselves from Russia-related activities and incorporating them into a recusal acknowledgment system designed to prevent U.S.-person participation in Russia-related contracts;

b. Assigning a senior compliance manager to manage the integration of Cameron into Schlumberger's compliance program;

c. Implementing an automatic block and review on all Russia-related orders; and

d. Implementing a software enhancement requiring end-users be identified for all transactions.

(2) Cameron cooperated with OFAC during the investigation by submitting detailed documentation, responding appropriately to OFAC's requests, and entering into tolling agreements.

Schlumberger Rod Lift, Inc.

On September 27, 2021, OFAC announced a $160,000 settlement with Schlumberger Rod Lift, Inc. ("SRL"), a Texas-based company, formerly a subsidiary of Schlumberger Lift Solutions LLC ("SLS"), itself a U.S. subsidiary of Schlumberger Limited ("Schlumberger") of Curacao, Netherlands, settling its potential civil liability for an apparent violation of OFAC's now-repealed Sudanese Sanctions Regulations ("SSR"), 31 C.F.R. § 538.206. OFAC determined that SRL's conduct was non-egregious and not voluntarily self-disclosed.

In August 2014, SLS acquired the assets of another Texas-based company and hired employees of the acquired company as part of the acquisition. Between December 2015 and April 2016, three of these U.S.-person employees facilitated the sale and shipment of oilfield equipment from a Canadian subsidiary of Schlumberger to a Chinese joint venture, in which Schlumberger held a 50% interest, for onward delivery to Sudan. All three employees were aware that the goods were destined for Sudan prior to arranging for shipment. Further, the employees were aware that U.S. sanctions at the time prohibited the sale of Schlumberger goods and provision of services to Sudan. In December 2015, the U.S. employees received an email requesting a price quote for oilfield equipment from Schlumberger's joint venture in China, for delivery to a customer in Sudan. Shortly after the email request, the employees received internal communications clearly stating that Sudan was a sanctioned country and referencing Schlumberger's internal Trade and Customs Compliance policies. Over the next several months, SRL employees, the Chinese joint venture, and the Canadian subsidiary exchanged emails to arrange and facilitate the sale and shipment of the goods.

Aggravating Factors

(1) The SRL employees that engaged in the violative transaction were explicitly informed that Sudan was under comprehensive U.S. sanctions and that they were not to engage in business with Sudan. They received emails and attended a training that communicated prohibitions on activities related to Sudan;

(2) The SRL employees that engaged in the violative transaction knew or had reason to know that the goods for which they were facilitating shipment would be exported to Sudan; and

(3) The conduct occurred not long after Schlumberger received, in August 2015, a Finding of Violation from OFAC regarding the facilitation of trade with and the exportation of goods to Iran and Sudan. The apparent violation occurred when Schlumberger was subject to a Plea Agreement with DOJ related to prior sanctions violations involving Sudan.

Mitigating Factors

(1) Schlumberger fully cooperated with OFAC's investigation, including submitting thorough documentation, providing timely responses to OFAC's requests, and entering into a tolling agreement; and

(2) Schlumberger engaged in remedial efforts, including removal of personnel involved in the apparent violation, and SRL (now Lufkin Rod Lift, Inc.) is in the process of enhancing its compliance program.

NewTek, Inc.

On September 9, 2021, OFAC announced a $189,483 settlement with NewTek, Inc. ("NewTek"), a developer and supplier of live production and 3D animation hardware and software systems headquartered in San Antonio, Texas. NewTek entered into the agreement to settle its potential civil liability for 52 apparent violations of the Iranian Transactions and Sanctions Regulations ("ITSR") that resulted from NewTek's exports of goods, technology, and services from the United States to third-country distributors that it knew or had reason to know were specifically intended for companies and individuals in Iran. OFAC determined that NewTek's conduct was non-egregious and voluntarily self-disclosed.

Between approximately December 2013 and May 2018, NewTek exported 49 products from the United States to two third-country distributors with knowledge or reason to know its products were intended specifically for a reseller located in Iran. The Iranian reseller sold three of the exported products to Islamic Republic of Iran Broadcasting ("IRIB"), which was an entity on OFAC's List of Specially Designated Nationals and Blocked Persons ("SDN List") at the time of the relevant exports. Moreover, on at least three occasions, NewTek provided support, software updates, reseller training, or other services in support of sales to customers located in Iran.

NewTek authorized distribution of its products to the Iranian reseller under two successive distributor agreements. The first distributor agreement authorized the distribution and support of NewTek's products in the "Middle East" region, which NewTek was informed specifically included Iran. The second distributor agreement specifically authorized the distribution of NewTek products in several countries comprising the Middle East sales territory, which explicitly included Iran. Accordingly, NewTek's conduct constituted apparent violations of the ITSR §§ 560.204 and 560.206, as well as apparent violations of Executive Order 13628 of October 9, 2012,[5] with respect to the three products provided to IRIB. The total value of the transactions constituting the apparent violations is $583,024, and the profits associated with the product sales that constituted the violations amounted to approximately $61,070.

Aggravating Factors

(1) NewTek demonstrated reckless disregard for U.S. sanctions requirements by entering into arrangements with two third-party distributors to specifically authorize distribution and support of its goods in Iran, knowing that relevant sanctions regulations generally barred dealings with Iran and relying on a mistaken understanding that its indirect dealings were permissible;
(2) NewTek possessed actual knowledge of the conduct leading to the apparent violations. NewTek employees throughout all levels within the company, including managers and members of NewTek's four-member executive board, possessed direct knowledge and/or reason to know that NewTek products were exported to distributors intended specifically for sale to an Iranian reseller and to end users in Iran.
(3) The sale of NewTek products to resellers and customers located in Iran harmed U.S. sanctions objectives by facilitating access to NewTek products and support services by

[5] Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions With Respect to Iran, Exec. Order No. 13,628, 77 Fed. Reg. 62,139 (Oct. 12, 2012).

resellers and users in Iran, including an Iranian electronics company that was part of the reseller network, and to an entity on the SDN List.

Mitigating Factors

(1) The total amount and volume of payments underlying the apparent violations was not significant compared to NewTek's overall revenue. Moreover, NewTek, a relatively small company, had not received a Penalty Notice or Finding of Violation from OFAC in the five years before the earliest date of the transactions giving rise to the apparent violations.

(2) NewTek took the following remedial actions:
   a. Established export controls and sanctions compliance policies and procedures;
   b. Hired a Director of Compliance;
   c. Provided compliance training to employees in sales, marketing, shipping, service, and compliance personnel;
   d. Obtained formal export classifications from the U.S. Department of Commerce confirming that NewTek's products are properly designated EAR99 for export control purposes;
   e. Implemented bulk name screening against the SDN List of its product registrants and current and pending distributors; and
   f. Implemented geo-IP blocking measures to restrict individuals located in Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine from downloading or registering NewTek products.

(3) NewTek substantially cooperated with OFAC's investigation into the apparent violations.

First Bank SA and JC Flowers & Co.

On August 27, 2021, OFAC announced a $862,318 settlement with First Bank SA ("First Bank"), located in Romania, and its U.S. parent company, JC Flowers & Co. ("JC Flowers"), settling potential civil liability for First Bank's processing of transactions in apparent violation of OFAC's Iran and Syria sanctions programs. OFAC determined that the apparent violations were voluntarily self-disclosed and non-egregious. Specifically, three categories of payment gave rise to the apparent violations:

1) Processing U.S. Dollar Payments for Individuals or Entities Located in Iran

Between March 2, 2016, and December 5, 2018, First Bank processed 34 outgoing payments totaling $991,246 through U.S. banks on behalf of Iranian customers of First Bank and in which the end user of the commercial transaction was in Iran. These transactions constituted an indirect exportation of financial services to Iran and caused U.S. financial institutions to export financial services to Iran, in apparent violation of the ITSR, 31 C.F.R. §§ 560.203 and 560.204.

2) Processing U.S. Dollar Payments for Individuals or Entities Located in Syria

Between July 15, 2016, and December 6, 2018, First Bank processed 36 outgoing payments totaling $1,061,104 through U.S. banks for which the trade finance documentation showed that the importers were in Syria. These transactions constituted an indirect exportation of financial services to Syria and caused U.S. financial institutions to export financial services to Syria, in apparent violation of the Syrian Sanctions Regulations ("SYSR"), 31 C.F.R. §§ 542.205 and 542.207.

3) Processing Euro-Denominated Payments to Iran as a Foreign Subsidiary of a U.S. Company
In June 2018, JC Flowers acquired a majority ownership interest in First Bank, thereby making First Bank an entity majority-owned by a U.S. person and, therefore, subject to the prohibitions of ITSR § 560.215. From October 17, 2018, to March 4, 2019, First Bank processed 28 Euro-denominated payments worth a total of $1,536,840 outside the U.S. financial system involving Iranian parties and interests where there was no applicable authorization or exemption, and with actual knowledge or reason to know that the payments were for Iranian parties. Accordingly, these transactions constituted apparent violations of ITSR § 560.215.

Aggravating Factors

(1) First Bank demonstrated a reckless disregard for U.S. sanctions regulations by failing to implement appropriate controls to comply with applicable U.S. regulations with respect to payments it processed (i) with a sanctions nexus that transited the U.S. financial system, or (ii) after the bank became a foreign subsidiary of a U.S. person. Moreover, First Bank failed to implement adequate internal controls necessary to ensure transactions with a U.S. sanctions nexus would be escalated to management for additional review, as provided in its existing compliance policy;
(2) First Bank had actual knowledge or reason to know that it was processing payments on behalf of persons in Iran and Syria because finance and trade documents in its possession referenced those countries; and
(3) First Bank conferred $3,589,189 in economic benefit to persons in Iran and Syria thereby undermining the integrity of the ITSR and SYSR and their associated policy objectives for at least three years.

Mitigating Factors

(1) First Bank and JC Flowers had not been issued a Penalty Notice or Finding of Violation in the five years before the earliest date of the transactions giving rise to the apparent violations.
(2) First Bank and JC Flowers cooperated with OFAC's investigation by conducting a historical lookback and entering into a tolling agreement with OFAC.
(3) First Bank and JC Flowers represented to OFAC that they undertook several remedial measures in response to the apparent violations, and following its change of ownership and the attendant enhanced commitment by JC Flowers to ensure compliance with the ITSR and SYSR, including:
    a. First Bank (i) updated its sanctions screening tool; (ii) terminated relationships with customers party to the subject transactions; and (iii) implemented enhanced diligence procedures to collect more information on the nature of transactions and potential for involvement with sanctioned jurisdictions, territories, or parties;
    b. First Bank implemented enhanced policies and procedures to address the relevance and applicability of U.S. sanctions regulations to the processing of transactions that transit the U.S. financial system, as well as those payments processed by an entity owned by a U.S. person;
    c. First Bank more than doubled its compliance staffing overseeing sanctions and related issues to provide more sources toward enhanced screening and monitoring;

d. First Bank conducted additional sanctions training with staff, and First Bank, following approval by its Supervisory Board, issued a new global sanctions policy; and
e. As part of the agreement with OFAC, First Bank and JC Flowers have undertaken to continue their implementation of these and other commitments.

Bank of China (UK) Limited

On August 26, 2021, OFAC announced a $2,329,991 settlement with Bank of China (UK) Limited ("BOC UK"), a London-based financial service provider, settling its potential civil liability for processing 111 transactions in apparent violation of OFAC's now-repealed SSR, 31 C.F.R. § 538.205. OFAC determined that BOC UK's self-identified apparent violations were voluntarily self-disclosed and did not constitute an egregious case.

Between September 4, 2014, and February 24, 2016, BOC UK exported financial services from the U.S. by processing 111 commercial transactions valued at $40,599,184 through the U.S. financial system on behalf of parties in Sudan.

As the result of an internal investigation, BOC UK conducted a review to identify Sudan-related transactions that identified two customers who had engaged in Sudan-related transactions that BOC UK processed via U.S. correspondent banks. However, with respect to both customers, BOC UK's internal customer database included no reference to Sudan in their name or address fields. As a result, transactions processed by BOC UK for those customers through U.S. banks did not include any references to Sudan. BOC UK's staff's failure to recognize underlying account and transactional documentation indicating ties to Sudan resulted in these compliance deficiencies.

Aggravating Factors

(1) BOC UK demonstrated a reckless disregard for U.S. sanctions requirements when, despite having access to account and transactional information indicating a connection to Sudan, BOC UK processed transactions for entities in Sudan through the U.S. financial system in contravention of the bank's existing policies and procedures;
(2) Certain individuals at BOC UK were aware that the payments were related to entities in Sudan;
(3) For at least one and a half years, BOC UK conferred economic benefit to Sudan, a then comprehensively sanctioned country, by processing 111 outgoing payments amounting to approximately $40.6 million; and
(4) BOC UK, a commercially sophisticated financial institution, routinely processes transactions internationally.

Mitigating Factors

(1) BOC UK had no prior sanctions history and had not received a Penalty Notice or Finding of Violation from OFAC in the five years before the earliest date of the transactions giving rise to the apparent violations.
(2) BOC UK self-identified the apparent violations and cooperated with OFAC's investigation by conducting a lookback review and entering into a statute of limitations tolling agreement.

(3) BOC UK represented to OFAC that it had taken several remedial measures since identifying the apparent violations, including:
    a. Establishing an executive-level committee tasked with implementing compliance policies and procedures, which ultimately reports to the Board of Directors;
    b. Conducting an annual enterprise-wide sanctions risk assessment by business line that incorporates risk monitoring and internal audit testing, and integrates input from external consultants;
    c. Implementing a centralized customer due diligence function firm-wide to strengthen internal controls;
    d. Customizing firm-wide sanctions compliance training for staff based on the employee's tenure and business line; and
    e. Enhancing policies and procedures to better address U.S. sanctions regulations applicable in processing payments through the United States.

Payoneer Inc.

On July 23, 2021, OFAC announced a $1,400,301 settlement with Payoneer Inc. ("Payoneer"), a New York-based online money transmitter and provider of prepaid access. Notably, OFAC determined that although Payoneer only submitted voluntary self-disclosures for 19 of the 2,241 apparent violations, the apparent violations do not constitute an egregious case.

Between February 2013 and February 2018, Payoneer violated six OFAC sanctions programs[6] when it processed 2,260 transactions totaling $802,117 for parties in jurisdictions subject to sanctions and on behalf of sanctioned individuals on OFAC's SDN List.

Specifically, Payoneer processed 2,241 payments for its corporate customers and card-issuing financial institutions located in the sanctioned jurisdictions of Crimea region of Ukraine, Iran, Sudan, Syria, and nineteen payments on behalf of individuals on the SDN List. Internal testing, audit, and screening failures resulted in Payoneer's processing of the transactions despite compliance policies that prohibited the practice as far back as June 2015. Notably, Payoneer's screening algorithms permitted close matches to SDN List entries not to be flagged. Payoneer also did not screen for Business Identifier Codes even when SDN List entries included them. In busy periods, Payoneer automatically released flagged and pending payments without review. Additionally, Payoneer failed to monitor IP addresses or flag addresses in sanctioned jurisdictions.

Aggravating Factors

(1) Payoneer did not exercise a minimal degree of caution or care for its sanctions compliance obligations when, as a result of deficient sanctions compliance processes that persisted for years, it allowed persons on the SDN List and persons in sanctioned jurisdictions to open accounts and transact;

[6] Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine, Exec. Order No. 13,685, 79 Fed. Reg. 77,357, §§ 1(a)(iii), 2 (Dec. 24, 2014); Zimbabwe Sanctions Regulations, 31 C.F.R. § 541.201; Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. § 544.201; Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.204;Sudanese Sanctions Regulations (now repealed), 31 C.F.R. § 538.205; Syrian Sanctions Regulations, 31 C.F.R. § 542.207.

(2) Payoneer had reason to know billing, shipping, and IP addresses, the location of the users it subsequently identified as located in jurisdictions and regions subject to sanctions; and
(3) The transactions in question undermined six different sanctions programs.

Mitigating Factors

(1) Payoneer senior management immediately filed a voluntary self-disclosure upon discovering potential sanctions compliance issues and cooperated with the OFAC investigation;
(1) Payoneer did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) Payoneer terminated the conduct that led to the transactions in question and undertook the following remedial measures in order to minimize the risk of recurrence of similar conduct in the future:
    (a) Replaced its Chief Compliance Officer, retrained all compliance employees, and hired new compliance positions focused on testing;
    (b) Introduced financial institution alias names and BIC codes to its screening software and implemented an automatic process triggering manual review of payments or accounts that match entries on the SDN List;
    (c) Enabled the screening of names, shipping and billing addresses, and IP information associated with account holders to identify jurisdictions and regions subject to sanctions;
    (d) Began flagging pending transactions by filter instead of allowing them to complete during periods of backlog; and
    (e) Implemented daily reviews of identification documents uploaded to Payoneer, and a rule engine that stops payments with identification indicating jurisdictions and regions subject to sanctions.
(3) Payoneer committed to continue its implementation of these and other compliance measures.

Alpha Laval Inc.

On July 19, 2021, OFAC announced a $16,875 settlement with Alfa Laval Inc. (“AL US”), a Richmond-based subsidiary of Alfa Laval AB. Notably, OFAC determined that although AL US did not submit a voluntary self-disclosure for the apparent violations, its apparent violations did not constitute an egregious case.

Between May 2015 and March 2016, AL US’ Pennsylvania-based subsidiary, Alfa Laval Tank, Inc. (“AL Tank”), violated section 560.208 of the ITSR when it referred an Iranian business opportunity to its foreign affiliate in the United Arab Emirates (“U.A.E.”), thus facilitating a transaction that would be prohibited if performed by U.S. persons. AL Tank also violated sections 560.204 and 560.206 of the ITSR when it exported U.S.-origin products to a foreign affiliate with knowledge or reason to know that the products were intended for supply, transshipment, or re-exportation to Iran.

Specifically, in May 2015, Alborz Pakhsh Parnia Company ("Alborz"), an Iranian distributor of oil products, sent AL Tank an inquiry about buying its Gamajet brand automated storage tank

cleaning machines. In the communication, Alborz explicitly stated it was located in Iran. AL Tank's portfolio manager for tank cleaning equipment responded with a recommendation for AL Tank products, pricing information, product descriptions, and an offer to prepare a quote.

In August 2015, AL Tank forwarded the Alborz inquiries to a tank cleaning portfolio manager at Alfa Laval Denmark ("AL Denmark") asking for a contact who could handle an Iran-related request. AL Denmark recommended contacting U.A.E. subsidiary of Alfa Laval AB based in Dubai, Alfa Laval Middle East Ltd. ("AL Middle East").

A series of emails between AL Tank and AL Middle East discussed whether AL Tank could quote or sell items from the U.S. to Iran. The correspondence ultimately led to the formation of a conspiracy by AL Middle East, Iran-based Alfa Laval Iran Co. Ltd. ("AL Iran"), a Dubai-based company ("Dubai company"), and Alborz to re-export AL Tank products from the U.S. to Iran, and to actively mislead AL Tank into believing that its products were destined for an end-user in the U.A.E.

Despite the conspiracy to deceive AL Tank with regards to the Iranian end-user, AL Tank failed to heed or largely ignored multiple warning signs that its products were at risk of diversion to Iran. In February 2016, AL Tank responded to an Alborz email containing "technical questions" about AL Tank Gamajet cleaning units. The subject line of the email read "Gamajet for Alborz Pakhsh Parnia Company." On the same day, AL Tank sent AL Middle East a "Gamajet Quotation Invoice" identifying the end-user as Iran. When AL Tank later asked AL Middle East who the end-user for the Gamajet order was, AL Middle East responded that the end-user was the Dubai company. In March 2016, AL Tank exported two Gamajet cleaning machines and accessories to the Dubai company. The machines, valued at $18,585, were then re-exported by the Dubai company to Alborz in Iran.

OFAC separately settled with AL Middle East for its role in the conspiracy and export-related transactions.

Aggravating Factors

(1) By failing to heed multiple warning signs that the end-user of its products was located in Iran, AL Tank recklessly violated the ITSR; and
(2) AL Tank undermined the ITSR by referring an Iran-related business opportunity to a foreign affiliate that formed a conspiracy that succeeded in re-exporting Al Tanks U.S.-origin goods to Iran's energy sector.

Mitigating Factors

(1) None of the relevant Alfa Laval AB subsidiaries, including AL US, received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) AL US employed outside counsel to conduct an internal investigation, which led to the imposition of remedial measures, including additional in-person training to reinforce Alfa Laval's Export Control Policy, a thorough internal investigation, and adoption of enhanced review and screening processes; and
(3) AL US cooperated with the OFAC investigation.

Alpha Laval Middle East Ltd.

On July 19, 2021, OFAC announced a $415,695 settlement with Alfa Laval Middle East Ltd., a U.A.E. seller of energy industry equipment. Notably, OFAC determined that AL Middle East did not submit a voluntary self-disclosure for the apparent violations, and the apparent violations constitute an egregious case.

Between May 2015 and March 2016, AL Middle East conspired with companies based in the U.A.E. and Iran to export AL Tank's Gamajet brand storage tank cleaning units from the U.S. to Iran in violation of section 560.203(b) of the ITSR. AL Middle East also violated section 560.203(a) of the ITSR when it caused AL Tank to export $18,585 worth of goods indirectly from the U.S. to Iran.

Aggravating Factors

(1) AL Middle East willfully violated the ITSR when it conspired to re-export U.S.-origin goods to an Iranian end-user by obfuscating the end-user's identity from its U.S. affiliate, AL Tank, causing AL Tank to violate the ITSR;
(2) AL Middle East's Sales Manager formed and participated in the conspiracy that resulted in the re-export of U.S.-origin goods to Iran, and several AL Middle East and AL Iran managers had actual knowledge of the re-export in question; and
(3) AL Middle East undermined the ITSR by circumventing U.S. sanctions and conferring an economic benefit to Iran's energy sector.

Mitigating Factors

(1) None of the relevant Alfa Laval AB subsidiaries, including AL US, received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) AL Middle East, through AL US, employed outside counsel to conduct an internal investigation, which led to remedial measures, including disciplinary action against those implicated in the re-export of U.S.-origin goods to Iran, a thorough investigation, adoption of enhanced review and screening processes for Iran-related transactions at AL Middle East, and additional in-person training to reinforce Alfa Laval's Export Control Policy; and
(3) AL Middle East, through AL US, cooperated with the OFAC investigation.

MoneyGram Payment Systems, Inc.

On April 29, 2021, OFAC announced a $34,329 settlement with MoneyGram Payment Systems, Inc. ("MoneyGram"), a Dallas-based global payments company.

Between March 2013 and June 2020, MoneyGram violated multiple sanctions programs[7] when it processed 359 transactions totaling $105,627 on behalf of approximately 40 individuals on the SDN List and two individuals who initiated commercial transactions involving Syria.

[7] Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R § 598.203; Narcotics Trafficking Sanctions Regulations, 31 C.F.R. § 536.201; Syrian Sanctions Regulations, 31 C.F.R. § 542.207; Democratic Republic of the Congo Sanctions Regulations, 31 C.F.R. § 547.201; Central African Republic Sanctions Regulations, 31 C.F.R. § 553.201; Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. § 544.201.

SDN List Transactions
MoneyGram's transactions on behalf of individuals on the SDN List occurred between March 2013 and April 2016, when MoneyGram provided money transfer services to the U.S. Department of Justice's Federal Bureau of Prisons ("BOP"), which allowed inmates to send and receive funds into and out of their personal commissary accounts. Until January 2015, MoneyGram failed to screen inmates against the SDN List despite being aware that blocked inmates could receive payments. At the time, MoneyGram incorrectly believed that the BOP program did not require screening of inmates in federal prison against the SDN List. Even after MoneyGram began screening the inmates' transactions, it continued to process transactions on behalf of blocked inmates due to human and technological errors, including screening and fuzzy logic failures.

Syria Transactions
The two individuals who initiated commercial transactions to Syria were able to do so because MoneyGram analysts incorrectly determined that the transactions qualified as noncommercial, personal remittances.

Aggravating Factors
(1) MoneyGram was aware that incarcerated blocked persons could receive payments into their commissary accounts but failed to screen beneficiaries against the SDN List because it misunderstood its due diligence obligations; and
(2) MoneyGram is a large and complex international financial institution.

Mitigating Factors
(1) Most of the 359 transactions were destined for blocked persons in the custody of the United States who would have probably been eligible for a license;
(2) MoneyGram did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(3) MoneyGram cooperated with OFAC's investigation;
(4) MoneyGram discovered the violations through ongoing efforts to strengthen its compliance program and immediately self-disclosed them to OFAC; and
(5) MoneyGram took strong remedial actions, including:
    (a) Implementing new compliance procedures, which include enhanced screening and improved mechanisms for monitoring and resolving sanctions-related alerts;
    (b) Screening for BOP-related transactions and denying services to commissary accounts of known blocked persons;
    (c) Requiring that the inmate name, rather than just the inmate account number, be included in the transaction data;
    (d) Introducing additional training to its agent network to increase the quality of data collected by agents; and
    (e) Adding 128 employees to its Compliance Department in 2016, appointing a new Chief Compliance Officer, and heavily investing in compliance-related functions.

SAP SE

On April 29, 2021, OFAC announced a settlement agreement with SAP SE ("SAP"), a software company headquartered in Germany, and a civil penalty of $2,132,174. The settlement involved 190 apparent violations that occurred between June 2013 and January 2018 and resulted in the export of SAP software and related services to Iran. The transactions in question involved SAP cloud-based software subscription sales and SAP's exportation and sales of software and services to pass-through entities.

SAP Sales to Pass-Through Entities

The SAP settlement agreement with OFAC indicates that SAP violated section 560.204 of the ITSR when it sold SAP software by its third-party resellers ("SAP Partners") to pass-through entities due to several compliance shortcomings, including failures to: (1) screen for and block customer IP addresses based in Iran (*e.g.*, unable to identify the country in which SAP software was downloaded); (2) conduct sufficient due diligence on SAP Partners' connections to Iranian companies; and (3) adequately investigate whistleblower allegations.

Specifically, SAP exported software and related services from its servers in the U.S. to SAP Partners in Turkey, the U.A.E., Germany, and Malaysia. SAP Partners then resold SAP software licenses and related services to companies controlled by Iranian firms that provided the SAP software to Iranian end-users. SAP Partners also advertised commercial relationships with Iranian companies on their websites.

Additionally, SAP failed to adequately investigate whistleblower allegations it received between July 2011 and March 2016. The whistleblower allegations claimed that SAP software had been sold to Iranian front companies registered in the U.A.E., Turkey, and Malaysia. SAP later substantiated the allegations.

Cloud-Based Software Sales

The SAP settlement agreement with OFAC also highlights how SAP's failure to integrate its cloud business group subsidiaries ("CBGs") into its broader compliance structure helped make it possible for SAP's CBGs in the United States to sell cloud-based software subscription services to customers who then provided remote access to users in Iran in violation of section 560.204 of the ITSR.

In 2011, SAP began acquiring U.S.-based CBGs that operated internationally but lacked adequate export controls and sanctions compliance programs. Despite these compliance shortcomings, SAP did not require that the CBGs adopt SAP's existing compliance procedures. SAP opted instead to rely on its small and resource-strained Export Compliance Team ("ECT") to coordinate and enforce compliance processes for the CBGs. Several CBGs were resistant to adopting ECT processes and sanctions compliance, believing them to be unnecessary. The ECT reported these challenges to SAP's Germany-based compliance team but received limited support.

SAP Compliance Shortcomings

SAP conducted several internal audits of its export controls processes, including a 2006 audit warning that SAP risked violating U.S. export controls because SAP did not identify the country

to which the software and support products were being downloaded. Subsequent audits in 2007, 2010, and 2014, continued to identify gaps in SAP's export controls processes. Despite these audits, SAP did not implement geolocation IP address blocking for its download delivery portal until July 2015. Even then, some Iranian-affiliated pass-through entities were able to evade SAP's geolocation blocking controls by feigning IP addresses located in non-sanctioned jurisdictions.

SAP also received several whistleblower complaints as early as 2011, claiming that SAP Partners were selling SAP products to non-U.S. affiliates of Iranian companies. According to BIS, SAP did not adequately investigate those reports. SAP did not conduct on-site examinations of SAP Partners until late 2017, when it confirmed that certain SAP Partners sold SAP products to the pass-through entities.

Additionally, certain SAP and SAP Partner executives, including senior leaders at the SAP Partner located in the U.A.E., were aware that the pass-through entities had purchased the SAP software with the intent of using the software in Iran. Publicly available information posted on certain SAP Partners' websites publicized their commercial ties to Iranian companies.

Aggravating Factors

(1) SAP showed reckless disregard and failed to exercise a minimal degree of caution or care for U.S. economic sanctions. Specifically, SAP:
    (a) Ignored at least eight years of internal audits and warnings from compliance personnel that highlighted sanctions compliance risks and deficiencies that could lead to violations;
    (b) Failed to address whistleblower claims alleging sales to Iran; and
    (c) Allowed its CBGs to operate independent and inadequate compliance programs despite reports from the ECT notifying SAP headquarters of significant compliance deficiencies;
(2) SAP acted recklessly by having a compliance program that was not commensurate to its size and sophistication
    (a) SAP failed to implement adequate compliance procedures, such as the geolocation of IP addresses during screening; and
    (b) SAP failed to conduct an adequate degree of due diligence on its partners.
(3) SAP had direct knowledge or reason to know that SAP software and cloud services were being sold or used by entities and end-users in Iran;
(4) SAP's export of U.S. business enterprise software and services to Iran harmed U.S. sanctions program objectives and undermined U.S. policy objectives by providing an economic benefit of $3.9 million in leading business enterprise software to Iran; and
(5) SAP is a sophisticated software company with significant international operations and has numerous foreign subsidiaries.

Mitigating Factors

(1) SAP had no prior OFAC sanctions history and did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;

(2) SAP cooperated with OFAC's investigation by arranging OFAC interviews with SAP employees; and
(3) SAP took significant remedial actions, including:
    (a) Terminating all users associated with the third-country entities that provided software and services to Iran, and Iranian cloud services;
    (b) Terminating SAP partners who resold software to Iranian companies;
    (c) Blocking all downloads of SAP software and related services from Iran and other embargoed countries;
    (d) Implementing a risk-based export control framework for SAP Partners that requires a stringent review of proposed sales by a third-party auditor;
    (e) Developing and implementing an enhanced compliance program, including geolocation IP addresses screening;
    (f) Hiring more than six new employees responsible for export control and sanctions compliance; and
    (g) Terminating five employees who knowingly sold SAP products to Iran or failed to follow SAP internal policies prohibiting sales to embargoed countries.

Alliance Steel, Inc.

On April 19, 2021, OFAC announced a $435,003 settlement with Alliance Steel, Inc. ("Alliance"), a U.S.-based designer and manufacturer of prefabricated steel structures.

From October 2013 to October 2018, Alliance appears to have violated sections 560.201 and 560.206 of the ITSR on at least 61 occasions when it engaged with an Iranian engineering firm to import Iranian-origin engineering services.

Specifically, Alliance's Chief Engineer and Vice President of Engineering outsourced a significant portion of Alliance's engineering work to an Iranian engineering firm owned by his brother. At least 12 other members of Alliance senior management had actual knowledge that the subcontractor was an Iranian company. Alliance paid the Iranian company approximately $1,450,008 over the five-year period.

Aggravating Factors

(1) Alliance failed to exercise basic due diligence regarding transactions with an Iranian engineering firm, which was its only international business relationship;
(2) Alliance senior management had actual knowledge that Alliance was outsourcing engineering work to an Iranian company. Specifically, senior Alliance officials approved invoices and issued checks to the Iranian engineering firm; and
(3) Alliance harmed ITSR objectives by outsourcing engineering work to an Iranian company for at least five years, thereby conferring over $1 million in benefits to Iran.

Mitigating Factors

(1) Alliance did not receive a Penalty Notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) Alliance voluntarily self-disclosed its apparent violations, including the dealings with the Iranian company to OFAC, and cooperated with OFAC's investigation; and
(3) Alliance took remedial measures, including:

(a) Terminating ongoing work with, and payments to, the Iranian engineering company;
(b) Terminating the employee who initiated and oversaw Alliance's outsourcing transactions;
(c) Developing and implementing an export compliance policy, which requires that management provide training to staff and international contracting opportunities be approved by the company's president.

Nordgas, S.r.l.

On March 26, 2021, OFAC announced a $950,000 settlement with Nordgas S.r.L. ("Nordgas"), an Italian manufacturer and seller of components for gas boiler systems and applications. Notably, OFAC determined that (1) Nordgas did not submit a voluntary self-disclosure for the apparent violations, and (2) the apparent violations constitute an egregious case.

Between March 2013 and March 2017, Nordgas appears to have violated sections 560.203 and 560.204 of the ITSR, when it: (i) engaged in re-exportation, sale, or supply of 27 shipments of air pressure switches from the U.S. to a party in another country, with knowledge or reason to know, that the switches were ultimately destined to Iranian companies; and (ii) caused a U.S. company to indirectly export goods to Iran.

In May 2010, Nordgas ordered air pressure switches for gas boiler systems from a U.S. company and notified the U.S. company of its intent to re-export the switches to customers in Iran. In response, the U.S. company informed Nordgas that U.S. sanctions regulations prohibited it from exporting U.S.-origin goods if the end-users were Iranian entities. Nordgas, in turn, offered to sell the switches to alternate end-users in Italy. No immediate sale resulted, but the two companies eventually developed a commercial relationship.

In 2012, Nordgas successfully re-exported the U.S. company's air pressure switches to Iran by misrepresenting to the U.S. company that the end-user was Nordgas' Italian affiliate. Nordgas continued to re-export the U.S. company's goods to Iran for several years by using code words for Iran in correspondence and trade documentation. In one instance, Nordgas also asked that the U.S. company remove "Made in USA" labels from the switches to disguise their origin.

In 2016, the U.S. company offered to ship goods directly to Nordgas' Italian affiliate, the stated end-user, due to Nordgas' inability to process the export in a timely manner. Nordgas refused the offer, citing logistical issues.

Aggravating Factors

(1) Nordgas engaged in willful conduct when it re-exported U.S.-origin goods to as many as ten companies in Iran after being notified that the re-exportations would violate U.S. sanctions regulations;
(2) Nordgas management had reason to know of the deceptive conduct that gave rise to the apparent sanctions violations, and either failed to provide effective oversight of its employees and operations or chose to ignore prohibited trade practices; and
(3) Nordgas harmed the objectives of U.S. sanctions on Iran by supplying over $2.5 million worth of goods from the U.S. to Iran.

Mitigating Factors

(1) Nordgas did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) Nordgas stopped shipping goods from the U.S. to Iran and took remedial action, including:
    (a) Implementing a sanctions compliance program;
    (b) Agreeing to enhance compliance commitments in its OFAC settlement agreement, including a commitment to submit annual reports to OFAC for five years outlining how Nordgas is implementing the compliance commitments in the settlement agreement; and
(3) Nordgas cooperated with the OFAC investigation by submitting detailed and well-documented responses to OFAC's written information requests, and by agreeing to toll the statute of limitations.

UniControl, Inc.

On March 15, 2021, OFAC announced a $216,464 settlement with UniControl, Inc. ("UniControl"), a Cleveland-based manufacturer of process controls, airflow pressure switches, and boiler controls.

Between July 2013 and March 2017, UniControl exported to two European companies 21 shipments of air pressure switches, valued at $687,189, that were subsequently re-exported to Iran in apparent violation of section 560.204 of the ITSR.

UniControl had actual knowledge that the last two shipments of the 21 shipments would be re-exported to Iran. Additionally, the re-exports of the switches to Iran occurred largely because UniControl did not adequately respond to several warning signs presented by its European trade partners that its goods were being re-exported to Iran. The warning signs included:

- Customer Interest in Iranian Market.
- Inclusion of Iran in Authorized Sales Territory.
- Obfuscated End-User Request.
- Engagement with Iranian Nationals at European Trade Shows.
- Request to Remove "Made in USA" Label.

Aggravating Factors

(1) For the first 19 shipments, UniControl did not respond to several warning signs that its European trade partner was re-exporting its goods to Iran;
(2) For the first 19 shipments, UniControl senior leadership was aware or should have been aware that UniControl products were being re-exported to end-users in Iran;
(3) For the last two shipments, UniControl exported the switches with actual knowledge that the switches were to be re-exported to an end-user in Iran; and
(4) For the last two shipments, UniControl's senior leadership had actual knowledge that UniControl products were to be re-exported to an Iranian end-user.

Mitigating Factors

(1) UniControl is a modest-sized company with no prior sanctions history with OFAC, and UniControl did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(2) UniControl had stopped all shipments to its European trade partners at the time of its disclosure to OFAC;
(3) UniControl cooperated with the OFAC investigation by submitting detailed and well-documented correspondence describing the apparent violations, and entered into two tolling agreements with OFAC; and
(4) UniControl invested in and enhanced its trade compliance procedures by:
    (a) Hiring outside counsel to assist in strengthening its sanctions compliance and export policies and procedures;
    (b) Requiring customers to sign end-user and end-use certificates to ensure that buyers do not resell UniControl products to prohibited end-users;
    (c) Requiring end-user certificates from secondary and tertiary buyers of re-exported UniControl products; and
    (d) Adding a Destination Control Statement to the footer of trade documents.

BitPay, Inc.

On February 18, 2021, OFAC announced a $507,375 settlement with BitPay, Inc. ("BitPay"), an Atlanta-based digital currency processing company. Notably, OFAC determined that although BitPay did not submit a voluntary self-disclosure for the apparent violations, the apparent violations do not constitute an egregious case.

Between June 2013 and September 2018, in apparent violation of various sanctions regulations,[8] BitPay processed 2,102 digital currency transactions valued at approximately $129,000 on behalf of individuals who, based on IP addresses and information available in invoices, were located in sanctioned jurisdictions, including the Crimea region of Ukraine, Cuba, North Korea, Iran, Sudan, and Syria.

Specifically, BitPay received digital currency payments on behalf of its merchants from buyers located in sanctioned jurisdictions. BitPay then converted the digital currency to fiat currency and relayed that currency to the merchants.

While BitPay screened its direct customers, the merchants, against OFAC's SDN List and ensured they were not located in sanctioned jurisdictions, BitPay did not screen its merchants' buyers' location data against the SDN list.

Aggravating Factors

(1) BitPay failed to exercise due caution or care for its sanctions compliance obligations when, for about five years, BitPay allowed individuals in sanctioned jurisdictions to

[8] Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. § 560.204 (2021); Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to the Crimea Region of Ukraine, Exec. Order No. 13,685, 79 Fed. Reg. 77357 (Dec. 24, 2014); Cuban Assets Control Regulations ("CACR"), 31 C.F.R. § 515.201 (2021); North Korea Sanctions Regulations ("NKSR"), 31 C.F.R. § 510.206 (2021); Sudanese Sanctions Regulations ("SSR"), 31 C.F.R. § 538.205; Syrian Sanctions Regulations ("SYSR"), 31 C.F.R. § 542.207 (2021).

transact with BitPay's merchants using digital currency despite having adequate information to screen those customers; and
(2) BitPay harmed the integrity of several U.S. sanctions programs by conferring $128,583 in economic benefit to persons in jurisdictions subject to OFAC sanctions.

Mitigating Factors

(1) BitPay implemented sanctions compliance controls as early as 2013, including due diligence and sanctions screening on merchant customers;
(2) BitPay compliance training emphasized that BitPay did not permit merchant sign-ups from Cuba, Iran, Syria, Sudan, North Korea, and Crimea, or transactions with sanctioned individuals and entities;
(3) BitPay was a small business at the time of the apparent sanctions violations and did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(4) BitPay cooperated with OFAC's investigation;
(5) BitPay ceased processing digital currency transactions involving buyers located in sanctioned jurisdictions and took remedial actions, including:
    (a) Blocking IP addresses that appear to originate in Cuba, Iran, North Korea, and Syria;
    (b) Confirming the physical and email addresses of merchants' buyers listed on merchant invoices if BitPay identifies a sanctioned jurisdiction address or email top-level domain; and
    (c) Launching "BitPay ID," a new customer identification tool required for merchants' buyers who wish to pay a BitPay invoice of $3,000 or more. As part of BitPay ID, the merchant's customer must provide an email address, proof of identification, and a photo.
(6) As part of the settlement agreement with OFAC, BitPay will continue the implementation of these and other compliance commitments.

PT Bukit Muria Jaya

On January 14, 2021, OFAC announced a $1,016,000 settlement with PT Bukit Muria Jaya ("BMJ"), a paper products manufacturer located in Indonesia. Notably, OFAC determined that although BMJ did not submit a voluntary self-disclosure for the apparent violations, the apparent violations do not constitute an egregious case.

In apparent violation of section 510.212 of the North Korea Sanctions Regulations ("NKSR"), arising from its exportation of cigarette paper to the Democratic People's Republic of Korea ("DPRK"), BMJ caused U.S. banks to: (i) clear wire transfers to an SDN; (ii) export financial services to the DPRK; or (iii) otherwise facilitate export transactions that would have been prohibited if engaged in by U.S. persons in apparent violation of the NKSR.

Specifically, BMJ directed payments to its U.S. dollar ("USD") bank account at a non-U.S. bank, causing 28 wire transfers to clear through U.S. banks between March 2016 and May 2018. These payments were initiated by companies based in, or facilitating, the DPRK in exchange for BMJ's exports of cigarette paper. One of the companies was a pass-through entity in China that re-exported goods to OFAC-designated Korea Daesong General Trading Corporation while it was

operating under an alias. BMJ initially identified the DPRK companies on transactional documents, including invoices, packing lists, and bills of lading. At the request of its customers, BMJ later substituted the names of the DPRK companies with those of intermediaries located in third countries. BMJ's total exports to the DPRK were valued at approximately $959,111.

It should be noted that BMJ did not voluntary self-disclose the apparent violations, therefore the base civil monetary penalty was higher, resulting in the $1,016,000 penalty.

Aggravating Factors

(1) BMJ demonstrated reckless disregard for U.S. sanctions laws and regulations when it directed payments related to DPRK trade activity to its USD account at a non-U.S. bank;
(2) BMJ management had actual knowledge of the sales of cigarette paper to the DPRK and BMJ employees omitted the DPRK nexus from transactional documents; and
(3) BMJ harmed U.S. foreign policy objectives when it caused U.S. persons to convey economic benefits to the DPRK and an OFAC-designated person.

Mitigating Factors

(1) BMJ did not receive a Penalty Notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions giving rise to the apparent NKSR violations, and the transactions represent a small percentage of BMJ's overall business during the relevant time period;
(2) BMJ cooperated with OFAC's investigation by providing detailed and well-organized submissions in response to requests for information, and agreed to provide ongoing cooperation as a term of settlement; and
(3) BMJ's remedial response to the apparent violations, include ceasing all dealing with the DPRK and implementing a new sanctions and export control compliance program that:
    (a) Appoints a new head of the Compliance Department, who reports directly to BMJ's president;
    (b) Procures sanctions screening services from a third-party provider;
    (c) Adopts a formal written export control and sanctions policy that outlines U.S. sanctions compliance practices and educates employees on when to escalate issues to BMJ's compliance division for further evaluation;
    (d) Creates a know-your-customer process that provides for escalation and risk-based review, including background checks and consultation with external counsel; and
    (e) Requiring all trading companies or agents who purchase goods on behalf of other end-users sign an anti-diversion agreement that includes OFAC sanctions compliance commitments.

Union de Banques Arabes et Françaises

On January 4, 2021, OFAC announced an $8,572,500 settlement with Union de Banques Arabes et Françaises ("UBAF"), a bank registered in France that facilitates international trade finance.

Between August 2011 and April 2013, UBAF processed 127 transactions, totaling $2,079,339,944, in apparent violation of Syria-related sanctions established by two executive orders.[9]

UBAF's apparent violations include:

(1) The processing of 114 internal transfers on behalf of Syrian entities totaling $1,297,651,826 that were followed by approximately 114 corresponding funds transfers

through a U.S. bank. For 45 of the 114 internal transfers, UBAF processed a USD transfer between two of its clients—one sanctioned Syrian entity and one non sanctioned client—on UBAF's books. UBAF then processed at least one USD transfer on behalf of the non-sanctioned client that cleared through a U.S. bank. The transaction dates and amounts of that transfer were consistent with internal transfers on UBAF's books. For the remaining 69 of 114 internal transfers, UBAF conducted a foreign exchange ("FX") transaction with a sanctioned Syrian customer on UBAF's books, debiting an account in one currency and crediting the same sanctioned customer's account in another currency. UBAF then conducted a U.S.-cleared FX transaction with a non-sanctioned third party that was consistent with the original FX transaction involving the sanctioned customer; and

(2) The processing through a U.S. bank of 13 "back-to-back" letter of credit transactions or other trade finance transactions involving sanctioned Syrian parties. For the back-to-back letter of credit transactions, a sanctioned Syrian entity was either the beneficiary of export letters of credit or the applicant for import letters of credit that did not involve USD clearing. However, the intermediary entered into, or received, one or more corresponding USD letters of credit to purchase or sell the same goods. For the other trade finance transactions, UBAF either issued a USD-denominated letter of credit on behalf of a sanctioned party or confirmed a USD-denominated letter of credit issued by a sanctioned bank. UBAF then paid on the letter of credit through a U.S.-cleared transaction.

Aggravating Factors

(1) UBAF showed a reckless disregard for its U.S. sanctions compliance obligations when it continued to provide USD services to sanctioned Syrian parties after the August 2011 expansion of U.S. sanctions on Syria without properly identifying and managing the relevant sanctions compliance risks;
(2) UBAF management had actual knowledge of the financial services it was providing to sanctioned Syrian parties; and
(3) UBAF harmed the integrity of U.S. sanctions laws and policy objectives when it conferred economic benefit to U.S.-sanctioned parties.

[9] Blocking Property of the Government of Syria and Prohibiting Certain Transactions With Respect to Syria, Exec. Order No. 13,582, 76 Fed. Reg. 52,209 (Aug. 22, 2011); Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters, Exec. Order No. 13,382, 70 Fed. Reg. 38,565 (July 1, 2005).

Mitigating Factors

(1) Most of the transactions in question occurred in late 2011, following the implementation of Executive Order 13582 on August 18, 2011, which greatly expanded the scope of U.S. sanctions against Syria;
(2) UBAF maintained a compliance program at the time of the transactions in question;
(3) UBAF voluntarily self-disclosed the apparent violations to OFAC and cooperated with OFAC's investigation by entering into a tolling agreement and agreeing to extend the agreement multiple times;
(4) UBAF did not receive a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions in question;
(5) UBAF has represented to OFAC that it has significantly invested in, and enhanced, its compliance program and undertook multiple remedial actions, including:
    (a) Automatically adopting the sanctions compliance policies of UBAF's largest

shareholder, a large and sophisticated financial institution, and using the shareholder's filtering software and supplemental lists to screen transactions;
(b) Offering in-person and e-learning compliance training for all employees at onboarding and on a continuing basis;
(c) Completing a review of UBAF business lines, which resulted in the cancellation of services deemed to be pose high compliance risks, including exiting relationships with high-risk banks, exiting business with Sudan and Syria in all currencies, and closing a foreign subsidiary for risk-related reasons; and
(d) Establishing a Compliance Committee, composed of senior managers, which meets regularly to monitor promised actions by member departments.

TORRES LAW

INTERNATIONAL TRADE & NATIONAL SECURITY

Questions? Contact Us:

Call 202.851.8200 or 214.295.8473
Email Info@torrestradelaw.com

Sign up for our newsletter: www.torrestradelaw.com