



EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

February 1, 2021 - Volume 13, Issue 2



Department of Commerce Takes Action against Avnet Asia for Involvement in Illegally Transshipping Sensitive U.S. Commodities to China and Iran

January 29, 2021 Office of Congressional and Public Affairs

Settlement resolves allegations that Avnet Asia employees illegally exported various electronic components, controlled under the Export Administration Regulations, to China and Iran via Singapore.

Today, Kevin J. Kurland, performing the non-exclusive functions and duties of the Assistant Secretary for Export Enforcement, Bureau of Industry and Security (BIS) of the U.S. Department of Commerce, announced an Administrative Settlement of \$3.2 million (partially suspended) with Singapore-based Avnet Asia Pte. Ltd. (Avnet Asia), a global distributor of electronic components and related software. BIS alleged that Avnet Asia employees illegally exported various electronic components, controlled under the Export Administration Regulations (EAR), through Singapore to China and Iran, including to a company on the BIS Entity List.

Concurrently, the Department of Justice announced the unsealing of an indictment today charging Cheng Bo, also known as Joe Cheng, a 45-year-old national of the People's Republic of China, with participating in a criminal conspiracy from 2012-2015 to violate U.S. export laws by shipping U.S. power amplifiers to China. Additionally, Cheng's former employer, Avnet Asia, agreed to pay a financial penalty to the United States of \$1,508,000 to settle criminal liability for the conduct of its former employees, including Cheng. As part of a Non-Prosecution Agreement, Avnet Asia admitted responsibility for Cheng's unlawful conspiracy to ship export controlled U.S. goods with potential military applications to China, and also for the criminal conduct of another former employee who, from 2007-2009, illegally caused U.S. goods to be shipped to China and Iran without a license. This conduct violated the International Emergency Economic Powers Act.

(*Continued On The Following Page)

NEWSLETTER NOTES

- * Department...
- * In first call with ...
- * PRINCETON ...
- * Tranche 5 More ...
- * Senate confirms Antony Blinken as ...
- * Janet Yellen Confirmed By Senate,...
- * CFIUS Enforcement ...
- * Dive Brief:
- * Biden's Commerce ...
- * BIS IMPOSES ...
- * BIS website update ...
- * Department of Commerce T...
- * CBP Through the Years
- * OFAC Settles with PT Bukit Muria ...
- * OFAC Enters Into \$98,830 Settlement with BitGo, Inc. ...
- * OFAC Enters ...

"The national security of the United States is, and will always be, the top priority for the Bureau of Industry and Security's Office of Export Enforcement," said Kurland. "Today's order, and related Department of Justice actions, send a strong message that export compliance matters. Individuals and companies that violate the Export Administration Regulations can be criminally prosecuted, administratively fined, or both."

The BIS settlement resolved allegations that on 53 occasions between October 2007 and January 2014, Avnet Asia ordered, sold, forwarded, and/or transferred over \$1.2 million worth of items subject to the EAR or the Iranian Transactions and Sanctions Regulations with knowledge or reason to know that a violation of the EAR was intended or about to occur in connection with the items. Most of these items, classified under Export Control Classification Number 3A001, are subject to export controls for National Security and Anti-Terrorism reasons and are prohibited from export to Iran and China without the requisite government authorization. BIS also alleged that Avnet Asia ordered, sold, forwarded and/or transferred electronic components subject to the EAR to Wing Shing Computer Components Company (H.K.) Ltd., a party on the BIS Entity List, without the required BIS licenses.

BIS's mission is to advance U.S. national security and foreign policy objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. Among its enforcement efforts, BIS is committed to preventing U.S.-origin items from supporting Weapons of Mass Destruction (WMD) projects, terrorist activities, or destabilizing military modernization programs. For more information, please visit www.bis.doc.gov.

In first call with Putin, Biden pressed Russian president on arms control, Navalny arrest, White House official says

White House press secretary Jen Psaki said President Biden called Vladimir Putin and discussed a number of topics, including Ukrainian sovereignty, the poisoning of opposition figure Alexei Navalny, reports of Russian bounties on U.S. troops in Afghanistan and interference in the 2020 election.

"His intention was also to make clear that the United States will act firmly in defense of our national interests in response to malign actions by Russia," Psaki said.

PRINCETON UNIVERSITY RESOLVES ALLEGATIONS OF EXPORT LAW VIOLATIONS WITH ADMINISTRATIVE SETTLEMENT

Today, Kevin J. Kurland, performing the non-exclusive functions and duties of the Assistant Secretary for Export Enforcement, Bureau of Industry and Security (BIS) of the U.S. Department of Commerce, announced an administrative settlement of \$54,000 with Princeton University, located in Princeton, NJ. Princeton University voluntarily self-disclosed potential violations of the Export Administration Regulations (EAR) to BIS, and cooperated with the investigation that was conducted by the New York Field Office of BIS's Office of Export Enforcement (OEE). Princeton University also agreed to complete one external audit and one internal audit of its export compliance program.

"The Bureau of Industry and Security strongly encourages research institutions to maintain robust export compliance programs to prevent violations of the EAR," said Mr. Kurland. "If violations do occur, voluntarily self-disclosing the violations to BIS will help mitigate penalties imposed to protect U.S. national security."

This settlement resolves BIS's allegations that on 37 occasions between November of 2013 and March of 2018, Princeton University engaged in conduct prohibited by the EAR when it exported various strains and recombinants of animal pathogens from the United States to various overseas research institutions without the required export licenses. The items were controlled for Chemical and Biological Weapons reasons, and valued in total at approximately \$27,000.

"This action demonstrates that the Office of Export Enforcement will continue to leverage our unique authorities as enforcers and regulators of our nation's export control laws to investigate possible violations by research institutions and hold them accountable when appropriate," said Jonathan Carson, OEE Special Agent in Charge of the New York Field Office. "These laws are meant to keep the potential building blocks for chemical and biological weapons from proliferating across the globe."

BIS's mission is to advance U.S. national security and foreign policy objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. Among its enforcement efforts, BIS is committed to preventing U.S.-origin items from supporting Weapons of Mass Destruction (WMD) projects, terrorist activities, or destabilizing military modernization programs. For more information, please visit www.bis.doc.gov.

Tranche 5 More Chinese Communist Military Companies Released

Since the Department of Defense (DoD) began identifying CCMCs in June 2020 in response to [requests](#) to do so from members of Congress, it has identified 44 CCMCs in five “tranches.” They are listed on the DoD website at: [Tranche 1](#), [Tranches 2 & 3](#), [Tranche 4](#), and [Tranche 5](#). Tranche 5 was [published](#) on January 14, 2021 and identifies as CCMCs: Advanced Micro-Fabrication Equipment Inc. (AMEC); Luokong Technology Corporation (LKCO); Xiaomi Corporation; Beijing Zhongguancun Development Investment Center; GOWIN Semiconductor Corp; Grand China Air Co. Ltd. (GCAC); Global Tone Communication Technology Co. Ltd. (GTCOM); China National Aviation Holding Co. Ltd. (CNAH); and Commercial Aircraft Corporation of China, Ltd. (COMAC). These entities are [not](#) on the Military End User List or the Entity List.

The EO’s prohibitions regarding the entities in Tranches 1, 2, and 3 became effective on January 11, 2021. The prohibitions applicable to the entities in Tranche 4 will become effective on February 1, 2021, and the prohibitions applicable to the entities on Tranche 5 will become effective on March 15, 2021.

Senate confirms Antony Blinken as secretary of state in the Biden administration

Blinken served as deputy secretary of state in the Obama administration and is one of President Biden’s closest and longest-serving foreign policy advisers.

He would succeed Mike Pompeo as the nation’s top diplomat as the new administration faces numerous challenges from China, Iran, Russia and North Korea.

Janet Yellen Confirmed By Senate, Making History As First Female Treasury Secretary

Janet Yellen addresses an event last month introducing the incoming Biden administration's economic team in Wilmington, Del. Yellen is the first woman to lead the Treasury Department.

The Senate quickly confirmed Janet Yellen to be Treasury secretary on Monday, days after she won unanimous backing from both Democrats and Republicans on the Senate Finance Committee. Yellen will be the first woman to lead the Treasury Department and will spearhead the Biden administration's response to the coronavirus recession. The Senate confirmed her with an 84-15 vote.

CFIUS Enforcement Arm Looks for Chinese Involvement in US Tech Startups Via Review of Past Investments

[Jane Edwards](#) February 1, 2021

A new enforcement team within the [Committee on Foreign Investment in the U.S.](#) is reviewing previous startup investments to determine the possible involvement of Chinese investors in U.S. technology companies and identify potential national security risks, The Wall Street Journal reported Sunday. The CFIUS enforcement team is collaborating with the FBI to look for tech investments that pose a national security threat by using the bureau’s database of deals involving foreign investors and ranking those transactions based on a threat assessment intelligence agencies provide, according to former government officials and employees.

Sources said some of the preliminary inquiries by the enforcement team have run for months, while others have resulted in formal government investigations. They said they expect to see an increase in fines, divestment orders and other penalties later this year as a result of these investment reviews. A spokeswoman for President Joe Biden said the administration “will ensure that Cfius evolves into a 21st-century committee and is able to appropriately evaluate new and evolving risks.”

A senior official at the Department of the Treasury said the number of personnel at the agency working on CFIUS-related matters increased from about 12 in 2018 to approximately 70 employees. The Treasury oversees CFIUS and received \$40 million more in its budgets for 2020 and 2021, driving the expansion of the interagency committee.

Dive Brief:

Author: Chris Teale @chris_teale

- The advanced air mobility (AAM) sector could be [worth \\$115 billion by 2035](#), according to a new report, but a national strategy around regulations and public-private partnerships (P3s) is necessary to ensure success.
- The AAM industry, which includes electric vertical takeoff and landing (eVTOL) aircraft that can be used to move people and goods, could create 280,000 jobs in the commercial aircraft sector, according to new research from Deloitte and the Aerospace Industries Association (AIA). But the report warns that while the United States could be a world leader in deploying the technology, China, South Korea and Germany are also competing hard, and the U.S. must stay ahead.
- For the U.S. to remain competitive, the report calls for a comprehensive national strategy that creates a "clean and conducive policy environment" to ensure safety while certifying aircraft for use; ensure continued research, development and manufacturing in the necessary technology for AAM like batteries, artificial intelligence (AI) and 5G; and scale the market by building physical infrastructure, drives demand and positions the industry to export its goods globally.



Kristin Musulin / Smart Cities Dive

Biden's Commerce Pick, Raimondo, Voices Tough Line on China

WASHINGTON - President Joe Biden's pick to oversee the Commerce Department took a tough line on China in her confirmation hearing Tuesday, though she stopped short of singling out which Chinese companies should remain on a list that limits their access to advanced U.S. technology.

If confirmed, as expected, Rhode Island Gov. Gina Raimondo, a former venture capitalist, would be responsible for promoting opportunities for economic growth domestically and overseas.

Raimondo focused her testimony before a Senate panel Tuesday on the need to help those sectors of the economy and the workers hit hardest by the coronavirus pandemic.

"COVID has shined a light on the inequities in our economy," Raimondo said. "The president has been very clear, we're going to build back better and more equitably, and I strongly support that."

She would inherit a department that took actions during the Trump administration that heightened tensions with China, namely through tariffs and the blacklisting of companies by placing them on the U.S. government's so-called Entity List. U.S. companies need to get a license to sell sophisticated technology to companies on the list.

"China's actions have been anti-competitive, hurtful to American workers and businesses, coercive, and, as you point out, they're culpable for atrocious human rights abuses," Raimondo said in response to a question from Sen. Ted Cruz, R-Texas. "So whether it's the entities list, or tariffs, or countervailing duties, I intend to use all those tools to the fullest extent possible to level the playing field for the American worker."

When Cruz pressed Raimondo on whether certain companies would remain on the Entity List, Raimondo said she would consult with lawmakers, industry and allies and "make an assessment as to what's best for American national and economic security."

Raimondo similarly demurred on a question about the tariffs the Trump administration had placed on imported steel and aluminum in the name of national security. Those tariffs have raised costs for metal-using industries. She told Sen. Roy Blunt, R-Mo., that she would listen to him and manufacturers in his state and "take their needs into account."

(*Continued On The Following Page)

Sen. Jacky Rosen, D-Nev., also voiced concerns about tariffs the Trump administration enacted on solar panels, which Rosen said cost the country tens of thousands of solar jobs. Again, Raimondo said she would work with her and she didn't take a direct stand. "I understand it's time-sensitive and challenging and a lot of jobs are at stake," Raimondo assured her.

Raimondo was elected governor in 2014 and won reelection in 2018. She's expected to handily win a confirmation vote, but it's unclear when that vote will occur. Nominations pertaining to national security generally take precedent. The vote may also have to wait on former President Donald Trump's impeachment trial, which will dominate the Senate's attention starting the week of Feb. 8.

Sen. Roger Wicker, R-Miss., who chairs the commerce committee, wrapped up the hearing on an encouraging note, telling Raimondo, "I do not believe you will be serving as governor of the state of Rhode Island for very much longer."

Raimondo, 49, is the first woman elected governor of Rhode Island. She is a Rhodes Scholar and a graduate of Yale Law School who recalls her father losing his job at a Bulova watch factory in Providence to show she can connect with those worried about jobs in the U.S. being moved to other countries.

Much of her hearing was focused on regional issues, with lawmakers from coastal states focused on protecting valuable fishing industries and lawmakers for rural states calling for enhanced access to broadband. She confirmed her interest in working with them on those issues and emphasized the need to tackle climate change. She noted as governor that she oversaw construction of the nation's first offshore wind farm.

"Like President Biden, I know the climate crisis poses an existential threat to our economic security, and we must meet this challenge by creating millions of good, union jobs that power a more sustainable economy," Raimondo said.

The Commerce Department comprises a dozen bureaus and agencies, including the National Weather Service, the U.S. Census Bureau and the Minority Business Development Agency. If confirmed, Raimondo would oversee the work of more than 40,000 employees.

BIS IMPOSES ADMINISTRATIVE PENALTIES FOR SUBMISSION OF FALSE OR MISLEADING EXPORT INFORMATION INVOLVING RUSSIA

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY

January 27, 2021 Office of Congressional and Public Affairs

On January 27, 2021, Kevin J. Kurland, performing the non-exclusive functions and duties of the Assistant Secretary for Export Enforcement, Bureau of Industry and Security (BIS) of the U.S. Department of Commerce, announced an Administrative Settlement of \$540,000 (partially suspended) with Julian Demurjian of San Francisco, CA. BIS alleged that Mr. Demurjian and CIS Project, a company that Demurjian owned and operated, caused, aided, or abetted seven violations of the Export Administration Regulations (EAR). These seven alleged violations were in connection with the submission of false or misleading information of the values of telecommunications networking equipment controlled for national security, encryption, or anti-terrorism reasons and destined for Russia.

"The Bureau of Industry and Security will not tolerate exporters undermining the integrity of our export control system through the submission of false or misleading information," said Mr. Kurland. "The Office of Export Enforcement will continue applying the investigative resources and authorities necessary, including the imposition of administrative penalties, to protect and promote U.S. national security, foreign policy, and economic interests."

The BIS settlement resolved allegations that on six occasions between December 2014 and August 2015, Demurjian and CIS Project prepared invoices on CIS Project letterhead that significantly undervalued the items, and provided these invoices to a freight forwarder. The freight forwarder subsequently filed Electronic Export Information (EEI) containing the false value information in the Automated Export System for each of the shipments. The BIS settlement also resolved allegations that, in February 2015, Demurjian and CIS Project generated and provided to the freight forwarder an invoice on CIS Project letterhead that falsely undervalued the items so that the stated value did not exceed \$2,500, and thus did not appear to trigger an EEI filing requirement. To settle this matter, Mr. Demurjian agreed to a stated penalty of \$540,000, of which \$480,000 will be suspended for a two-year probationary period, and a two-year suspended denial of export privileges under the EAR.

(*Continued On The Following Page)

"Today's action demonstrates Export Enforcement's commitment to combating violations of export laws and regulations," said Special Agent in Charge John D. Masters of BIS's San Jose, CA Field Office.

"BIS has a compelling interest in ensuring that parties submit complete and accurate information to the U.S. Government in connection with their exports."

BIS's mission is to advance U.S. national security and foreign policy objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. Among its enforcement efforts, BIS is committed to preventing U.S.-origin items from supporting Weapons of Mass Destruction (WMD) projects, terrorist activities, or destabilizing military modernization programs. For more information, please visit www.bis.doc.gov.

BIS website update to list the UVL and MEU lists as separate electronic files

On January 28, 2021, BIS updated the EAR database on the BIS website to post Supplement No. 6 to part 744 – Unverified List and Supplement No. 7 to part 744 – 'Military End-User' (MEU) List as separate electronic files, similar to how the Supplement No. 4 to part 744 – Entity List is posted as a separate electronic file.

These changes to the BIS website are made solely to assist the public in more easily accessing those two supplements on the BIS website. No regulatory changes are made to the two supplements as part of this update of the BIS website.

Department of Commerce Takes Action against Avnet Asia for Involvement in Illegally Transshipping Sensitive U.S. Commodities to China and Iran

In this press release, the Bureau of Industry and Security (BIS) announces an Administrative Settlement of \$3.2 million (partially suspended) with Singapore-based Avnet Asia Pte. Ltd. (Avnet Asia), a global distributor of electronic components and related software. BIS alleged that Avnet Asia employees illegally exported various electronic components, controlled under the Export Administration Regulations (EAR), through Singapore to China and Iran, including to a company on the BIS Entity List

[Press Release](#)

CBP Through the Years

On [March 1, 2003](#), U.S. Customs and Border Protection became the nation's first comprehensive border security agency with a focus on maintaining the integrity of the nation's boundaries and ports of entry.

Before CBP, security, compliance and facilitation of international travel and trade were conducted by multiple organizations. The consolidation of these roles and responsibilities allowed CBP to develop seamless security procedures while ensuring compliance with the nation's immigration, health, and international trade laws and regulations.

In establishing CBP, its leadership ensured that the best traditions of its legacy agencies continued from:

U.S. Customs Service, which traced its original functions to [July 31, 1789](#), and noted its role as the progenitor of numerous federal bureaus and agencies. The Customs Service closed with the dawn of CBP, but its commissioner became the leader of CBP and the majority of its staff and responsibilities came to CBP.

Immigration inspectors, who traced their responsibilities to the establishment of the Office of the Superintendent of Immigration on [March 3, 1891](#).

Agriculture inspectors, who traced their roles to the passage of the Plant Quarantine Act on [Aug. 20, 1912](#).

Border Patrol agents, who brought their responsibility for maintaining the integrity of the U.S. borders as they have done since Congress authorized the hiring of Border Patrol personnel on [May 28, 1924](#).

In addition to this core of specialties and responsibilities present at CBP's founding, CBP also developed an air and marine monitoring capability with the formation of its third uniformed division, the Office of Air and Marine on [Jan. 17, 2006](#).

The uniformed ranks are only a portion of CBP's specialized corps. They are joined by forensic scientists, international trade specialists, public affairs officers and cadres of other specialists and employees who work together to make CBP's processes more secure, cost effective and efficient.

Because of the work of the people of CBP, the nation's borders and the American communities around them have never been more secure. But there is much more to be done. As CBP progresses into its second decade, the nation will see a fully integrated approach to international security, trade and travel that makes the world safer, facilitates international travel and trade, and drives the continuous improvement of CBP's operations.

<https://www.cbp.gov/about/history>

OFAC Settles with PT Bukit Muria Jaya for Its Potential Civil Liability for Apparent Violations of the North Korea Sanctions Regulations

PT Bukit Muria Jaya (BMJ), a paper products manufacturer located in Indonesia, has agreed to pay \$1,016,000 to settle its potential civil liability for 28 apparent violations that arose from its exportation of cigarette paper to the Democratic People's Republic of Korea (DPRK). BMJ directed payments for these exports to its U.S. dollar bank account at a non-U.S. bank, which caused U.S. banks to clear wire transfers related to these shipments, including shipments made to a blocked North Korean person. This settlement amount reflects OFAC's determination that BMJ's conduct was non-egregious and accounts for BMJ's remedial response. This case further highlights the risks to non-U.S. persons who involve the U.S. financial system in commercial activity with an OFAC-sanctioned country, region, or person.

Conduct Leading to the Apparent Violations

BMJ exported cigarette paper to entities located in or doing business on behalf of the DPRK, including to an intermediary in China that procured cigarette paper from BMJ on behalf of OFAC-designated Korea Daesong General Trading Corporation ("Daesong") while Daesong was operating under an alias.¹ BMJ initially referenced DPRK entities on its transactional documents, but at the request of its customers certain BMJ sales employees later replaced such references with the names of intermediaries located in third countries, including on invoices, packing lists, and bills of lading. The approximate commercial value of BMJ's exports to the DPRK was \$959,111.

BMJ directed payments for its DPRK-related exports to its U.S. dollar bank account at a non-U.S. bank. This caused 28 wire transfers related to such exports to clear through U.S. banks between March 2016 and May 2018. Accordingly, BMJ appears to have violated § 510.212 of the North Korea Sanctions Regulations, 31 C.F.R. part 510 (NKS), when it caused U.S. banks to: (i) deal in the property or interests in property of a Specially Designated National or Blocked Person; (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

§§ 510.201, 510.206, and 510.211 of the NKS (the "Apparent Violations").

After learning of its exposure to U.S. sanctions laws and regulations, BMJ represented that it ceased all dealings involving the DPRK and adopted a formal written sanctions policy and compliance procedures, as more fully described below.

(*Continued On The Following Column)

Penalty Calculations and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is \$8,621,816. OFAC determined that BMJ did not voluntarily self-disclose the Apparent Violations and that the Apparent Violations constitute a non-egregious case.

Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter is \$1,270,000.

The settlement amount of \$1,016,000 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be aggravating factors:

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

OFAC determined the following to be mitigating factors:

- (1) BMJ has not received a Penalty Notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the Apparent Violations, and the transactions giving rise to the Apparent Violations 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 consisting of representations that it has ceased all dealings with the DPRK and implemented a new sanctions compliance program that includes:

- A new head of the Compliance Department who reports directly to the company's president, and statements from the Chief Executive Officer to company employees encouraging them to report compliance concerns;
- Procurement of sanctions screening services from a third-party provider;

(*Continued On The Following Page)

- A formal written export control and sanctions policy that includes guidance for compliance with U.S. sanctions and identifies red flags to educate employees when to contact BMI's compliance division for further assessment;
- A know-your-customer process that provides for escalation and risk-based review, including consultation with external counsel or background checks, if heightened risks are identified; and
- A requirement that 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.

BMI's obligation to pay OFAC the settlement amount shall be deemed satisfied by BMI's payment of a greater amount in satisfaction of penalties assessed by the U.S. Department of Justice arising from the same course of conduct.

As described in OFAC's A Framework for Compliance Commitments (the "Framework"), many non-U.S. persons have engaged in violations of OFAC's regulations by causing U.S. persons to engage in prohibited transactions. All persons, including non-U.S. persons, engaged in international trade and commerce should be aware of sanctions prohibitions applicable to non-U.S. persons who involve U.S. persons in such transactions. These circumstances can arise when financial transactions that pertain to commercial activity with an OFAC-sanctioned country, region, or person are processed through or involve U.S. financial institutions. Involving a U.S. financial institution in such commercial activity—including the shipment of goods to or from a third-country to an OFAC-sanctioned country—may cause violations of OFAC regulations, such as the prohibited exportation or reexportation of services from the United States, or by U.S. persons, to a comprehensively sanctioned jurisdiction.

For companies engaged in trade with international partners, the absence of a risk-based sanctions compliance program may contribute to the likelihood of committing such a violation. This risk may be particularly acute when dealing with DPRK companies and individuals, or those who may be acting on their behalf, given the DPRK's widespread efforts to evade U.S. and international sanctions. On May 2, 2019, OFAC published the Framework in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use U.S.-origin goods or services, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at www.treasury.gov/ofac/enforcement.

For more information regarding OFAC regulations, please go to: www.treasury.gov/ofac.

OFAC Enters Into \$98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

BitGo, Inc. ("BitGo"), a technology company based in Palo Alto, California, that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services, has agreed to remit \$98,830 to settle its potential civil liability for 183 apparent violations of multiple sanctions programs (the "Apparent Violations"). As a result of deficiencies related to BitGo's sanctions compliance procedures, BitGo failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its non-custodial secure digital wallet management service. BitGo had reason to know that these users were located in sanctioned jurisdictions based on Internet Protocol (IP) address data associated with devices used to log in to the BitGo platform. At the time of the transactions, however, BitGo failed to implement controls designed to prevent such users from accessing its services. OFAC determined that BitGo did not voluntarily self-disclose the Apparent Violations and that the Apparent Violations constitute a non-egregious case.

This action emphasizes that OFAC sanctions compliance obligations apply to all U.S. persons, including those involved in providing digital currency services. As part of a risk-based approach, OFAC encourages companies that provide digital currency services to implement sanctions compliance controls commensurate with their risk profile.

Description of the Apparent Violations and the Conduct Leading to the Apparent Violations

Between approximately March 10, 2015 and December 11, 2019, BitGo processed 183 digital currency transactions, totaling \$9,127.79, on behalf of individuals who, based on their IP addresses, were located in sanctioned jurisdictions. The Apparent Violations related to BitGo's "hot wallet" secure digital wallet management service.¹ Individuals located in Crimea, Cuba, Iran, Sudan, and Syria signed up for "hot wallet" accounts and accessed BitGo's online platform to conduct digital currency transactions.

*(*Continued On The Following Page)*

*(*Continued On The Following Page)*

At the time of the Apparent Violations, BitGo tracked its users' IP addresses for security purposes related to account logins. BitGo, however, did not use this IP address information for sanctions compliance purposes. As a result, users located in Crimea, Cuba, Iran, Sudan, and Syria were able to create and use digital currency wallets on BitGo's platform and engage in digital currency transactions, despite BitGo's ability to identify the location of these users.

Prior to April 2018, BitGo allowed individual users of its secure wallet management services to open an account by providing only a name and email address. In April 2018, BitGo amended its practices to require all new accountholders to also verify the country in which they are located, but BitGo generally relied on each user's attestation regarding their location and did not perform additional verification or diligence on the location of its users. However, after learning of the Apparent Violations, in January 2020, BitGo implemented an OFAC Sanctions Compliance Policy ("OFAC Policy") and undertook significant remedial measures, as further described below. By failing to prevent users located in Crimea, Cuba, Iran, Sudan, and Syria to access and use its services to engage in digital currency transactions, BitGo apparently violated Executive Order 13685 of December 19, 2014, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine", the Cuban Assets Control Regulations, 31 C.F.R. §515.201; the Iranian Transactions and Sanctions Regulations, 31 C.F.R. §560.204; the Sudanese Sanctions Regulations, 31 C.F.R. §538.205 (SSR2); and the Syrian Sanctions Regulations, 31 C.F.R. §542.207.

Penalty Calculation and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is \$53,051,675. OFAC determined that BitGo did not voluntarily self-disclose the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter is \$183,000. The settlement amount of \$93,830 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be aggravating factors:

- (1) BitGo failed to exercise due caution or care for its sanctions compliance obligations when it failed to prevent persons apparently located in sanctioned jurisdictions to open accounts and send digital currencies via its platform as a result of a failure to implement appropriate, risk-based sanctions compliance controls; and
- (2) BitGo had reason to know that some of its users were located in sanctioned jurisdictions based on those users' IP address data, which it had separately obtained for security purposes.

*(*Continued On The Following Column)*

OFAC determined the following to be mitigating factors:

- (1) BitGo is a relatively small company and has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the apparent violations;
- (2) BitGo cooperated with OFAC's investigation into these apparent violations; and
- (3) BitGo represented that it has invested in significant remedial measures in response to the Apparent Violations and as part of its agreement with OFAC to implement compliance commitments intended to minimize the risk of recurrence of similar conduct in the future, including:
 - BitGo hired a Chief Compliance Officer and implemented its new OFAC Policy, which now applies to all BitGo's services;
 - BitGo implemented a new OFAC Policy that includes:
 - o A detailed overview of OFAC and relevant sanctions laws;
 - o The appointment of a compliance officer specifically responsible for implementing and providing guidance and interpretation on matters related to U.S. sanctions laws;
 - o IP address blocking, as well as email-related restrictions, for sanctioned jurisdictions;
 - o Periodic batch screening;
 - o Recordkeeping procedures for all financial records and documentation related to sanctions compliance efforts;
 - o A review and, where appropriate, update of end-user agreements to ensure that customers are aware of, and comply with, U.S. sanctions requirements; and
 - o A review of screening configuration criteria on a periodic basis.
 - BitGo screens all accounts, including "hot wallet" accounts, against OFAC's Specially Designated Nationals and Blocked Persons List, including blocked cryptocurrency wallet addresses identified by OFAC. BitGo has also conducted a retroactive batch screen of all users;
 - BitGo routinely reviews its OFAC Policy and updates its procedures, as appropriate; and
 - BitGo employees are required to certify that they have reviewed and understand BitGo's

Continue Here:

https://home.treasury.gov/system/files/126/20201230_bitgo.pdf

OFAC Enters Into \$8,572,500 Settlement with Union de Banques Arabes et Françaises for Apparent Violations of Syria-Related Sanctions Program

Union de Banques Arabes et Françaises (“UBAF”), a bank based in France that facilitates trade finance between Europe and the Middle East, North Africa, sub-Saharan Africa, and Asia, has agreed to remit \$8,572,500 to settle its potential civil liability for 127 apparent violations of Syria-related sanctions (the “Apparent Violations”). Between August 2011 and April 2013, UBAF operated U.S. dollar (USD) accounts on behalf of sanctioned Syrian financial institutions and indirectly conducted USD business on behalf of these institutions through the U.S. financial system. In particular, the majority of the Apparent Violations involved UBAF’s processing of internal transfers on behalf of Syrian entities that were followed by corresponding funds transfers through a U.S. bank. The remaining Apparent Violations were either “back-to-back” letter of credit transactions or other trade finance transactions involving sanctioned parties, all of which were processed through a U.S. bank. This settlement amount reflects OFAC’s determination that UBAF’s Apparent Violations were non-egregious and voluntarily self-disclosed.

Description of the Apparent Violations and the Conduct Leading to the Apparent Violations

In total, UBAF engaged in 127 Apparent Violations. This includes UBAF’s processing of 114 internal transfers on behalf of Syrian entities totaling \$1,297,651,825.61 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 own books. UBAF then processed one or more USD transfers on behalf of the non-sanctioned client that cleared through a U.S. bank and whose transaction dates and amounts correlated closely to the related internal transfers reflected 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 correlated closely with the original FX transaction involving the sanctioned customer.

(*Continued On The Following Column)

The remaining 13 Apparent Violations were either “back-to-back” letter of credit transactions or other trade finance transactions involving sanctioned Syrian parties, all of which were processed through a U.S. bank. For the back-to-back letter of credit transactions, a sanctioned Syrian entity was the beneficiary of export letters of credit or the applicant for import letters of credit that did not involve USD clearing, but 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 and paid on the letter of credit through a U.S.-cleared transaction.

Accordingly, between August 2011 and April 2013, UBAF processed 127 transactions, totaling \$2,079,339,943.52, in apparent violation of Executive Order 13582 of August 17, 2011, “Blocking Property of the Government of Syria and Prohibiting Certain Transactions with Respect to Syria” (“E.O. 13582”), and Executive Order 13382 of July 1, 2005, “Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters” (“E.O. 13382”). UBAF’s actions during this time period demonstrated knowledge of OFAC sanctions laws, but it incorrectly believed that avoiding direct USD clearing on behalf of sanctioned parties was sufficient; thus, the bank acted recklessly by failing to exercise a minimal degree of caution or care in accounting for the risks associated with continuing to provide USD-based services to OFAC-sanctioned parties.

Penalty Calculation and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is \$4,158,679,887.04. OFAC determined, however, that UBAF voluntarily self-disclosed the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC’s Economic Sanctions Enforcement Guidelines (“Enforcement Guidelines”), the base civil monetary penalty amount applicable in this matter is \$15,875,000. The settlement amount of \$8,527,500 reflects OFAC’s consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be aggravating factors:

- (1) UBAF demonstrated 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 that providing those services posed to the bank;
- (2) UBAF management had actual knowledge of the conduct giving rise to the Apparent Violations; and

*(*Continued On The Following Page)*

(3) UBAF conferred significant economic benefit to U.S.-sanctioned parties and caused significant harm to the integrity of U.S. sanctions programs and their associated policy objectives.

OFAC determined the following to be mitigating factors:

- (1) The majority of the Apparent Violations occurred in late 2011, following the implementation of Executive Order 13582 on August 18, 2011, which significantly expanded U.S. sanctions against Syria;
- (2) UBAF had a compliance program in place at the time of the apparent violations;
- (3) UBAF voluntarily self-disclosed the Apparent Violations to OFAC and cooperated with OFAC's investigation of the Apparent Violations by entering into a tolling agreement and agreeing to extend the agreement multiple times;
- (4) UBAF has not received 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 Violations; and
- (5) UBAF has represented to OFAC that it has invested substantial resources in improving its compliance program and undertook several remedial measures in response to the Apparent Violations. These measures include:

- UBAF adopted a new Financial Security Charter on September 12, 2013, based on the compliance policies of its largest shareholder, a large and sophisticated financial institution, at the invitation and with the support of the shareholder. UBAF automatically adopts all of this financial institution's sanctions policies, and also utilizes its filtering software and supplemental lists to screen transactions. This includes screening the client database, an anti-stripping module, negative news research, risk database research, vessel screening, and country screening.
- UBAF set up a Compliance Committee, composed of senior managers, which meets regularly to monitor follow-up on promised actions by member departments.

*(*Continued On The Following Column)*

For more information regarding OFAC regulations, please visit:
<http://www.treasury.gov/ofac>.

Information concerning the civil penalties process is discussed in OFAC regulations governing the various sanctions programs and in 31 C.F.R. Part 501. On November 9, 2009, OFAC published as Appendix A to Part 501, the Economic Sanctions Enforcement Guidelines. See 74 Fed. Reg. 57,593 (Nov. 9, 2009). The Economic Sanctions Enforcement Guidelines, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at
<http://www.treasury.gov/ofac/enforcement>

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use U.S.-origin goods or services, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Reproduction for private use or gain is subject to original copyright restrictions.

“Difficult roads often lead to beautiful destinations.”