

March 16, 2020

OFAC Cites the Use of U.S.-Origin Software and U.S. Network Infrastructure in Reaching a Nearly \$8 Million Settlement with a Swiss Commercial Aviation Services Company

On February 26, 2020, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") announced a \$7,829,640 settlement agreement with Geneva-based Société Internationale de Télécommunications Aéronautiques SCRL ("SITA"), to settle its potential civil liability for 9,256 apparent violations of the Global Terrorism Sanctions Regulations ("GTSR").¹ The case involved the alleged provision of commercial services and software subject to U.S. jurisdiction for the benefit of certain airline customers designated by OFAC as specially designated global terrorists ("SDGTs") between April 2013 and February 2018.²

This action is significant because it appears to be OFAC's first public enforcement action asserting OFAC jurisdiction over a scenario where the only U.S.-nexus was the provision of U.S.-origin software by SITA, a non-U.S. person, with knowledge that designated persons would benefit from the use of that software. It also appears to be OFAC's first public enforcement action finding U.S. jurisdiction where the only U.S. touchpoint for certain apparent violations was U.S.-based network infrastructure (essentially, a server), even though the services involved were otherwise provided outside of the United States.

The Apparent Violations

OFAC determined that SITA appears to have violated §§ 594.201 and 594.204³ of the GTSR by providing commercial services and software subject to U.S. jurisdiction to SDGTs. SITA provides telecommunications and information technology services to the civilian air transportation industry. SITA has members across the globe, and provides services to both members and non-members. The company also has a number of U.S. subsidiaries that develop and support certain SITA group services.⁴ These services include reservation-related services, networking services, planning services, messaging services, and ancillary services to travel, such as tracking software. Certain of these services are provided from the United States.

OFAC initiated its investigation upon the discovery that Mahan Air ("Mahan"), Syrian Arab Airline ("Syrian"), and Caspian Air ("Caspian"), three SDGTs, were member-owners of SITA, and may have received or benefitted from services or technology subject to United States jurisdiction. During the course of the investigation, SITA identified two additional SDGTs, Meraj Air ("Meraj") and Al-Naser Airlines ("Al-Naser"), which had been provided services by SITA as well.

The OFAC settlement describes the apparent violations as resulting from three services provided by SITA for the benefit of the SDGT airlines:

- Type B messaging (TBM) – a messaging service enabling communication with other parties in the aviation industry. All messages at issue in the settlement were routed through a “mega-switch” in Atlanta, Georgia and were originated from or destined for an SDGT airline, or other parties that were themselves providing services to those airlines. The “mega-switch” is a network switch that essentially functions as a server that receives, processes, and forwards messages to and from SITA members.
- Maestro DCS Local – U.S.-origin process management software that allows users to manage processes such as check-in and baggage management.
- WorldTracer – a baggage tracking system hosted on U.S. servers and maintained by SITA’s U.S. subsidiaries.

OFAC found that “[t]hese services and software were subject to U.S. jurisdiction because they were provided from, or transited through, the United States or involved the provision of U.S.-origin software with knowledge that customers designated as SDGTs would benefit from the use of that software.” In the case of TBM and WorldTracer, these apparent violations can be characterized as SITA initiating or causing the prohibited exportation of services from the United States. However, with respect to Maestro DCS Local, the only U.S. nexus appears to be the U.S.-origin of the software, which was determined by OFAC to be provided by SITA with knowledge that SDGTs would benefit from the use of such software.

According to OFAC, SITA had previously taken measures to comply with U.S. economic sanctions laws and regulations and had terminated certain services provided to airlines designated as SDGTs. It had also taken steps to mitigate sanctions compliance risks following a global risk assessment undertaken by management in 2016.⁵ OFAC reported that the company acknowledged that, prior to this assessment, its compliance program was not “comprehensive” or “detailed” and was “primarily reactive.” As a result, when airlines were designated as SDGTs, SITA allegedly reviewed its agreements with those airlines and terminated the provision of certain services. However, due to deficiencies in its compliance program, SITA nonetheless continued to provide the above-mentioned services to the SDGTs, as it apparently did not perceive those services to be subject to U.S. jurisdiction.

Factors Affecting OFAC’s Penalty Determination

OFAC determined that SITA did not voluntarily self-disclose the apparent violations and that the apparent violations constitute a non-egregious case. The statutory maximum civil monetary penalty amount for the apparent violations was \$2,453,077,327,⁶ and the base penalty amount was \$13,384,000.

In reaching the settlement amount, OFAC considered a number of aggravating factors, including that “SITA had actual knowledge that it was providing services and software directly or indirectly to SDGTs” and that the company is a “commercially sophisticated entity that operates in virtually every country in the world.”

OFAC also noted various mitigating factors, including that the transactions at issue “represented a small percentage of SITA’s overall business” and that the company implemented extensive remedial efforts and enhancements to its compliance program, customer and supplier screening, and its expulsion of Mahan, Syrian, and Caspian from the organization.” OFAC enumerated the following remedial actions undertaken by SITA:

- “Established a global trade board to expressly monitor and vet compliance risk involving customers, suppliers, and other parties”;
- “Established a trade compliance committee to act as an information sharing and advisory body in relation to trade and sanctions law matters that affect SITA or its members”;
- “Appointed a dedicated global head of ethics and compliance that has focused its efforts on developing and improving the compliance function as a whole”;
- “Implemented new sanctions legal compliance reviews when onboarding new customers and suppliers, and when extending or adding new products or services to existing customers in sanctioned countries”;
- “Updated and created new compliance policies and guidelines to bring awareness of sanctions compliance issues to the business”;
- “Committed to monitoring and auditing its messaging, Maestro, and WorldTracer systems periodically to verify that they are not being used to support SDGT airlines”; and
- “Required all new SITA employees to attend sanctions compliance training; and required sanctions compliance training for all SITA employees every year, and on an annual basis.”

Implications

The SITA case heralds OFAC’s apparent novel position that non-U.S. companies risk violating U.S. sanctions by using U.S.-origin software for the benefit of persons targeted by U.S. sanctions, even absent any other U.S. nexus. OFAC did not elaborate on the basis for this position beyond stating that the software was subject to U.S. jurisdiction because it “involved the provision of U.S.-origin software with knowledge [by SITA] that customers designated as SDGTs would benefit from the use of that software.” While many of OFAC’s jurisdiction-based sanctions programs contain a prohibition on re-exports of U.S. origin goods, the GTSR contains no such explicit prohibition. The GTSR prohibit “U.S. persons” from the “making of any

contribution or provision of funds, goods, or services by, to, or for the benefit of any [SDGT].”⁷ OFAC appears to view SITA’s dealings in U.S.-origin software, outside of the United States, as involving U.S. persons for the purposes of the GTSR. It is possible that OFAC took the view that SITA’s use of U.S.-origin software for the benefit of SDGTs *caused* an unnamed U.S. software exporter to violate the GTSR, particularly if SITA knew when it obtained the software that it would be used to benefit SDGTs or if there were ongoing updates or patches downloaded from the United States to support the software.

The SITA settlement also appears to represent OFAC’s first public enforcement action where a portion of the apparent violations were based solely on the fact that network infrastructure supporting the activities of a non-U.S. person in its dealing with sanctioned parties was physically located in the United States. Although OFAC has previously taken the position that such U.S.-based “back office” support could trigger a violation of its sanctions programs (*see, e.g.*, its authorization of the provision of certain automated back office services in support of transactions with Iran in the context of the Iran nuclear deal), the SITA settlement may signal a more aggressive enforcement stance against non-U.S. persons availing themselves of U.S.-based resources in connection with their dealings with sanctioned persons or jurisdictions. Prior public OFAC enforcement actions focused on U.S.-located involvement in a non-U.S. company’s activities have generally involved situations where U.S.-based personnel were performing an active support function—such as providing technical support—in connection with sanctioned transactions. For example, in the *Schlumberger* case, OFAC pursued an enforcement action related to a U.S. subsidiary’s support of its non-U.S. affiliates’ business with sanctioned countries, including the provision of technical expertise to repair equipment located in sanctioned countries.⁸ As cautioned by OFAC in its 2019 guidance regarding compliance, non-U.S. companies with integrated global operations that include the United States should take steps to ensure any activities they engage in are compliant with OFAC’s sanctions programs.⁹

While non-U.S. companies are generally not prohibited by U.S. sanctions from engaging in transactions with sanctioned persons or jurisdictions, the SITA case is an important reminder that virtually any U.S. nexus to such transactions can trigger a sanctions enforcement action. Companies should consider the following lessons from the SITA action:

1. Non-U.S. companies that provide U.S.-origin software or provide services that are routed through the United States, including through U.S.-based servers or other network infrastructure, should strongly consider having in place policies, procedures, and systems to prevent the provision of this software or services to sanctioned jurisdictions or parties. This is consistent with SITA’s post-settlement commitment to “monitor[] and audit[] its messaging, Maestro, and WorldTracer systems periodically to verify that they are not being used to support SDGT airlines.” Such measures would generally involve sanctioned party screening, as well as measures to prevent business with sanctioned jurisdictions.
2. Non-U.S. companies that knowingly conduct business with sanctioned jurisdictions or parties—which was the case in SITA’s situation—should carefully assess this business for any U.S. nexus,

including any reliance on U.S.-origin goods or software, U.S.-based back office services, or U.S. subsidiaries or personnel. Where a non-U.S. person knowingly does business with sanctioned jurisdictions or parties, OFAC would likely have heightened expectations that the company would be diligent in its risk analysis and procedures to avoid any prohibited touchpoints with the United States.

3. Similarly, in considering the policies, procedures, and systems discussed above, U.S. and non-U.S. companies alike should consider taking affirmative steps to prevent the diversion by their customers of U.S.-origin goods or services to sanctioned jurisdictions or parties, or other ways in which they may be dealing indirectly with sanctioned jurisdictions or parties. As demonstrated by OFAC in the recent *Apollo Aviation* settlement, sanctions contractual provisions will not, by themselves, shield a company from liability, and companies should consider implementing compliance procedures and monitoring that extend beyond point-of-sale and continue throughout the entire contractual relationship.¹⁰
4. Finally, OFAC noted in its web notice that the aviation industry is high-risk from a sanctions compliance perspective and that OFAC had previously issued an advisory warning of deceptive practices in the aviation industry. Although the referenced advisory was issued in the context of OFAC's Iran and Syria sanctions programs, OFAC noted that "participants in the civilian aviation industry should be aware that other jurisdictions and persons subject to OFAC sanctions may engage in similar deceptive practices."¹¹ Companies would be well-served to assess OFAC advisories and other guidance for potential lessons learned and application to their operations, even where such guidance is ostensibly focused on a specific industry or sanctions program.

We will continue to monitor sanctions developments and look forward to providing you with further updates.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jicarey@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

Rachel M. Fiorill
+1-202-223-7346
rfiorill@paulweiss.com

Karen R. King
+1-212-373-3784
kking@paulweiss.com

Law Clerk Jacob A. Braly contributed to this client alert.

¹ See U.S. Dep't of Treasury, OFAC, "Enforcement Information for February 26, 2020," available [here](#) ("OFAC Web Notice").

² Unlike most other OFAC sanctions programs, the GTSR do not exempt from its prohibitions transactions ordinarily incident to travel pursuant to the Berman Amendment to the International Emergency Economic Powers Act. The Berman Amendment likely accounts for the fact that OFAC did not pursue as violations SITA's dealings with Iran Air, which is designated solely under the Iran Transactions Sanctions Regulations (the "ITSR"). It also may explain why OFAC did not pursue reexport violations in connection with SITA's apparent reexport of software and services to sanctioned countries under the relevant country sanctions programs (e.g., the ITSR with respect to Mahan Airlines, which is based in Iran).

³ See 31 C.F.R. part 594. Section 201 prohibits transactions involving blocked property in which a SDGT has an interest; section 204 prohibits the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any SDGT. OFAC interprets this prohibition to apply to services performed in the United States or by U.S. persons. 31 C.F.R. §594.406.

⁴ OFAC Web Notice at 1.

⁵ *Id.*

⁶ The statutory maximum penalty is calculated by multiplying the number of apparent violations by the per transaction statutory maximum penalty (currently \$302,504 *per* transaction under the International Emergency Economic Powers Act). The statutory maximum penalty is equivalent to the base penalty in egregious matters with no voluntary self-disclosure. In these matters, high-volume industries (e.g., internet services, internet commerce, logistics, and financial services) can easily face substantial base penalty amounts driven, in large part, by the number of transactions involved.

⁷ 31 C.F.R. §594.204.

-
- ⁸ U.S. Dep't of the Treasury, Office of Foreign Assets Control, *Finding of Violation* (Aug. 7, 2015), available [here](#).
- ⁹ See U.S. Dep't of the Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), available [here](#); Paul, Weiss, *OFAC Issues Guidance on Sanctions Compliance Programs and Flags "Root Causes" Underlying Prior Enforcement Actions* (May 14, 2019), available [here](#).
- ¹⁰ See Paul, Weiss, *OFAC Enforcement Action against U.S. Aviation Company Shows the Importance of Ongoing Monitoring over the Course of a Contractual Relationship* (Dec. 9, 2019), available [here](#).
- ¹¹ OFAC Web Notice at 4.