Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lessons From SAP's Multiagency Illegal Export Penalty

By **Robert Slack and Julia Kuelzow** (May 18, 2021, 5:10 PM EDT)

Robert Slack

Julia Kuelzow

On April 29, three U.S. agencies — the Office of Foreign Assets Control, the U.S. Department of Commerce and the U.S. Department of Justice — announced the global resolution of apparent U.S. sanctions violations by SAP SE, a German software company.

The settlement agreements with OFAC and Commerce, and the nonprosecution agreement with the DOJ, highlight sanctions risks specific to the cloud and software industry, and provide insight on the U.S. government's compliance program expectations for companies that sell software and services online.

What Happened

According to the agency notices, between 2010 and 2018, SAP supplied software and cloud-based services from the U.S. to third parties, with reason to know that the offerings would be provided to users or customers in Iran. The violations transpired in two ways.

Sales of Software Through Pass-Through Entities

SAP sold software licenses and maintenance services to SAP resellers located in Turkey, the United Arab Emirates, Germany and Malaysia, which in turn sold the licenses and services to third parties for end use in Iran. Iranian end users then downloaded SAP software, updates or patches from the company's servers in the U.S.

The agencies noted that SAP failed to prevent downloads of its software from IP addresses associated with Iran, even though internal audits recommended the adoption of IP address geolocation screening. SAP also failed to conduct sufficient due diligence on its resellers, many of which publicized ties with Iranian companies on their websites.

Cloud Services

SAP's cloud business group subsidiaries allowed 2,360 users in Iran to access U.S.-based cloud services. SAP became aware, through due diligence and audits, that its subsidiaries lacked adequate compliance controls over its cloud offerings, but did not take appropriate or timely remedial action.

SAP voluntarily disclosed the issues to the three agencies, cooperated with investigators, and made significant changes to its export controls and sanctions compliance program by (1) implementing an IP-based geo-block, (2) deactivating user accounts of cloud-based services in Iran, (3) auditing and suspending resellers that sold to Iranian entities, and (4) involving the export compliance team in any new acquisitions, among other improvements.

All told, SAP paid $8.3 million in penalties and fines to resolve these cases, including a $3.2 million fine to Commerce and the disgorgement of $5.1 million in ill-gotten proceeds to the DOJ. OFAC suspended its separate penalty of $2.1 million.

Of course, those figures do not reflect the full cost of investigating and remediating the issues at hand. According to the DOJ, SAP spent over $27 million on remediation, which was noted as an important mitigating factor in the case. SAP also faces continued compliance and audit requirements under the terms of its settlement agreements.

Compliance Expectations and Lessons Learned

The SAP case is the latest sanctions enforcement action dealing with the provision of goods or services over the internet. As with prior announcements, we can glean a few lessons for the technology industry and for companies that conduct business online.

Geo-Blocking — Again

The SAP case is the latest reminder that the U.S. government expects technology companies to adopt effective geo-blocking of IP addresses associated with sanctioned jurisdictions. In its case summary, OFAC called out the particular need for an effective blocking solution when providing services indirectly through third parties.

U.S.-Based Servers are Subject to U.S. Rules

U.S. sanctions and export control laws have broad extraterritorial reach. This case highlights the fact that the provision of services and the download of software from U.S. servers are considered exports, and may require approval from OFAC and/or Commerce.

Non-U.S. companies should take note and consider their use of U.S. servers when assessing business opportunities that implicate destinations subject to U.S. sanctions. U.S.-based platforms should also consider whether customers' use of their services in sanctioned jurisdictions could create liability for the U.S. company providing the service.

Due Diligence on Intermediaries

The SAP case exemplifies how intermediary parties can create liability for a company under U.S. sanctions and export control rules. Appropriate due diligence, controls, and monitoring of distributors and resellers is a must in any industry, particularly when a U.S. company does not have full insight into the identity of the end users of its goods or services.

Intercompany Business Not Risk-Free

SAP allowed its subsidiaries to operate independently, although SAP knew, based on pre- and post-acquisition due diligence, and notification by SAP's U.S. compliance team, that those subsidiaries had insufficient sanctions compliance programs. Companies need to ensure that non-U.S. affiliates dealing in U.S. origin services or software maintain appropriate controls, especially after acquiring new entities.

Resourcing Export and Sanctions Compliance Teams

SAP relied on its U.S.-based compliance team to oversee the compliance of all of its cloud business group subsidiaries. However, the team received inadequate resources, lacked authority to manage the processes and encountered resistance from the subsidiaries. In its notice, OFAC emphasized that compliance teams must be resourced and empowered to implement compliance controls, when risks are identified.

Training

According to OFAC, SAP employees outside the U.S. oversaw the sale of U.S.-based offerings to Iran, and even traveled to Iran on a sales trip. Multinational companies with a U.S. presence should train all relevant employees on U.S. sanctions red flags so that these types of issues are spotted and appropriately reported.

Implement Audit Findings

SAP auditors highlighted the company's lack of IP address geo-blocking as a sanctions compliance risk as early as 2006, but the company did not implement effective controls until 2015. By failing to act in response to the audit findings, OFAC indicated that SAP "demonstrated reckless disregard and failed to exercise a minimal degree of caution or care" for U.S. economic sanctions and cited this failure as an aggravating factor in the case.

Voluntary Self-Disclosure Benefits

The agreements also demonstrate the potential benefit of voluntarily self-disclosing U.S. sanctions and export control violations to U.S. regulators. Notably, SAP's nonprosecution agreement with the DOJ marks the first voluntary disclosure of export and sanctions violations publicly resolved pursuant to the agency's new voluntary self-disclosure policy.

Under that policy, disclosure and cooperation result in a presumptive nonprosecution agreement and limitation on the penalty amount, absent any aggravating factors. SAP took advantage of similar voluntary self-disclosure provisions under OFAC's and Commerce's regulations, which provide for substantially reduced penalties for qualifying disclosures.

Concluding Thoughts

The SAP settlement underscores that companies selling U.S.-origin services and software should implement compliance controls suited to the nature of their business. Turning a blind eye to compliance considerations can lead to costly penalties later.

In this case, SAP failed to consider data indicating that end users may be located or operating in Iran, and lacked sufficient controls to ensure that indirect sales complied with U.S. rules. SAP also had several indications — between its own internal compliance team and audits — that its program, and its

subsidiaries' programs, had gaps, yet the company did not undertake sufficient due diligence to fully understand the issues or empower its compliance team to take remedial action.

Addressing compliance red flags can be difficult — it takes resources and commitment from a company. But doing so proactively, and early, prevents costly penalties and enforcement actions later on.

Robert Slack is a partner and Julia Kuelzow is an associate at Kelley Drye & Warren LLP.