The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 28, NO. 8 • AUGUST 2021

OFAC Enforcement Actions Highlight Risks to Software Providers and Money Services Businesses

By Michael Dawson, Ronald I. Meltzer, David M. Horn, Zachary Goldman, Semira Nikou, and Alina Lindblom

On April 29, 2021, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) announced two settlements of potential civil liability with two companies over their apparent violations of its regulations. The companies, MoneyGram Payment Systems, Inc. (MoneyGram) and SAP SE (SAP), operate in sectors of the economy—payments and software—that present unique sanction risks and compliance challenges.

The two settlements highlight many of those risks, such as the reliance on third-party resellers, the integration of newly acquired companies, and contracting with the US government. They are part of a trend of increased OFAC enforcement[1] and OFAC's communication of its compliance expectations through civil enforcement actions (which reinforce the guidance OFAC provided in its 2019 Framework for OFAC Compliance Commitments (Framework)). The SAP case is also notable because it is the first instance in which a company made a voluntary self-disclosure to, and entered into, a non-prosecution agreement (NPA) with the US Department of Justice (DOJ) pursuant to the 2019 Export Control and Sanctions Enforcement Policy for Business Organizations.

Companies should review these and other recent settlements to ensure that their compliance programs address the root causes of penalized companies' violations and adopt the types of internal controls recommended by OFAC.

SAP

German software company SAP, which provides enterprise application software and cloud-based services, reached an $8 million global settlement with OFAC, DOJ, the US Attorney's Office for the District of Massachusetts, and the US Department of Commerce Bureau of Industry and Security (BIS) for violations of the Iranian Transactions and Sanctions Regulations and the Export Administration Regulations. Of that amount, $2.13 million was paid to OFAC.[2]

SAP's apparent violations appear to have had two sources: (1) third-party resellers in Turkey, the United Arab Emirates, Germany, and Malaysia sold SAP software to third country companies that SAP referred to as "pass-through entities," which in turn sold licenses and services to companies in third countries that were either controlled by Iranian companies or that provided the SAP software to users in Iran; and (2) SAP's acquired cloud business group (CBG) subsidiaries in the United States sold cloud-based software subscription services to customers

that, in turn, granted access to their employees or customers located in Iran.

OFAC identified several shortcomings with SAP's compliance program. First, OFAC determined that SAP failed to screen its customers' Internet Protocol (IP) addresses, which resulted in SAP's inability to identify the country in which its software was downloaded. OFAC stated that SAP acted recklessly by not "instituting geo-location IP address screening for SAP software delivered from the United States." It also noted in its section on compliance considerations that screening processes "for global companies providing software products online, including through cloud-based services, direct downloads, or other such means . . . will generally include IP address identification and blocking capabilities and are especially important for companies that use sales models where engagement with the end-user is indirect."

Second, OFAC found that SAP failed to conduct proper due diligence on its third-party resellers. OFAC noted that such diligence could have revealed those entities' connections to Iran, including through public websites as well as investigations of whistleblower complaints.

Finally, OFAC determined that SAP failed to integrate CBG subsidiaries in a timely fashion—and allowed them to operate as standalone entities without integrating them into the company's broader compliance structure—despite pre- and post-acquisition due diligence revealing deficiencies in those entities' sanctions compliance programs. Instead, SAP relied on its small, under-resourced and under-empowered US-based Export Compliance Team to coordinate and enforce sanctions processes for the CBGs. But such processes "were not consistent across all the CBGs" as a result of technological challenges and the CBGs' own resistance to new sanctions compliance controls.

As a mitigating factor, OFAC found that SAP "substantially" cooperated with OFAC's investigation, including by arranging interviews with SAP employees, a notable form of cooperation that also earned SAP credit in its NPA with DOJ. Additionally, SAP took "significant remedial actions," including by terminating all users associated with the third-country entities that provided software and services to Iran, and Iranian cloud services; terminating commercial relationships with all third-party resellers involved in sales to Iranian companies; blocking software downloads in Iran and other comprehensively sanctioned jurisdictions; updating its export control framework to require a stringent review of proposed third-party reseller sales by a third-party auditor; implementing geolocation IP screening; hiring new employees responsible for export control and sanctions compliance; and terminating five employees who either knowingly engaged in sales to Iran or failed to adhere to SAP's internal policy prohibiting such sales.[3]

The NPA marks DOJ's first-ever resolution pursuant to its Export Control and Sanctions Enforcement Policy for Business Organizations (the Policy), published on December 13, 2019.[4] The Policy, while maintaining existing procedures for voluntary self-disclosure to regulatory agencies, encourages companies to voluntarily self-disclose to DOJ "all potentially willful violations of the statutes implementing the US government's primary export control and sanctions regimes." Importantly, the Policy states that a company will qualify for benefits under the Policy only if it self-reports to DOJ—and not if it does so to another regulatory agency (in contrast, OFAC may consider a company's voluntary self-disclosure to another agency as a voluntary self-disclosure for OFAC's purposes as well). Here, DOJ found that SAP had committed "serious offenses" affecting US national security, but that "the national security ramifications were tempered by SAP's voluntary self-disclosure, remediation, and cooperation."[5] Indeed, DOJ praised SAP for having conducted a thorough internal investigation, proactively identifying issues and facts of likely interest to DOJ and the US Attorney's Office for the District of Massachusetts, making regular presentations, voluntarily making employees located abroad available

for interviews, and identifying, investigating, and disclosing conduct that was outside the scope of the company's voluntary self-disclosures.

SAP must carry out a number of obligations under the NPA for a period of three years (or longer if DOJ determines that SAP violates or fails to fully perform any of its obligations). For example, SAP agreed to annually certify its compliance with the NPA and to cooperate with DOJ or other domestic or foreign law enforcement and regulatory authorities in any investigation of SAP, its subsidiaries, or its personnel relating to the conduct described in the NPA.

The NPA requires SAP to make extensive enhancements to its compliance program, to the extent it has not already done so. These enhancements include implementing an effective internal system for reporting sanctions or export control violations; conducting mandatory corporate ethics and export control training for all directors, officers, and other relevant employees of SAP and its subsidiaries; where applicable, informing partners, agents, consultants, and other third parties about their sanctions and export control obligations; auditing all newly acquired companies within 60 calendar days of acquisition to determine whether their ethics and export enforcement controls are adequate; promulgating an effective disciplinary system for all directors, officers, employees, agents, and business partners of SAP and its subsidiaries who are found to violate US sanctions or export controls; and promptly notifying DOJ in writing about possible criminal conduct relating to any suspected or attempted violations of US sanctions or export controls.

SAP also reached a settlement agreement with BIS, pursuant to which it is required to conduct internal audits of its compliance with US export control laws and regulations and produce audit reports to BIS for a three-year period.

MoneyGram

OFAC reached a $34,328.78 settlement with MoneyGram, a Texas-based global payments company, regarding the company's potential civil liability arising from apparent violations of multiple sanctions programs.[6] Specifically, from March 2013 to June 2020, MoneyGram processed 359 transactions totaling $105,627 on behalf of around 40 people on the Specially Designated Nationals and Blocked Persons (SDN) List.

What is notable about this case is that most of these apparent violations arose because MoneyGram provided money transfer services to DOJ's Federal Bureau of Prisons (BOP). The services allowed these SDNs, who were incarcerated in US federal prisons, to send and receive funds into and out of their personal commissary accounts.[7] OFAC found that MoneyGram knew that some of these inmates were on the SDN List but that the company mistakenly believed that it was not expected to screen them under the BOP program. MoneyGram identified the issue as part of a "compliance improvement program," but it continued to process transactions on behalf of blocked US inmates "due to other screening, technology, and fuzzy logic failures, as well as limited instances of human error."

While OFAC found that the statutory maximum civil monetary penalty applicable to the matter was over $30 million, a number of factors impacted the relatively low monetary penalty amount and OFAC's finding that MoneyGram's conduct was non-egregious. Notably, MoneyGram voluntarily self-disclosed the apparent violations to OFAC. Other factors include the following: the majority of the transactions destined for blocked persons in US custody would probably have been eligible for an OFAC license; MoneyGram cooperated with OFAC's investigation of the matter; MoneyGram discovered the apparent violations as part of its ongoing efforts to improve its sanctions compliance program; and the company represented to OFAC that it significantly improved its screening process and overall sanctions compliance program.

Sanctions Compliance Considerations

These two enforcement actions highlight several important takeaways about the risks that software and payments companies face, as well as OFAC's compliance expectations.

Cloud-based services providers should assess the adequacy of their sanctions compliance programs. OFAC emphasized in the SAP case that companies with global operations that provide software products online, including through cloud-based services, direct downloads, or other similar means, should implement a risk-based sanctions compliance program reflective of their "size and sophistication and appropriate to their marketing and operational structures." Such programs generally should include IP geo-blocking capabilities, especially for those relying on third-party vendors or distributors, or whose customers may provide the products to employees or other users.

Conduct pre- and post-acquisition due diligence. Through both the Framework and recent enforcement actions (see, for example, OFAC's recent settlement with Kollmorgen), OFAC has made it clear that it expects acquiring companies to conduct adequate due diligence on newly acquired subsidiaries and that compliance functions be integrated following an acquisition. To this end, compliance efforts should be sufficiently resourced and empowered to examine risks and implement appropriate controls, even (and perhaps especially) when encountering resistance from the new subsidiary.

Conduct counterparty due diligence. Both MoneyGram and SAP failed to adequately investigate information reasonably available to them—information that would have revealed a sanctions nexus. OFAC found that SAP had failed to conduct sufficient due diligence on its partners, which would have revealed their business with Iran. For example, it failed to adequately investigate whistleblower allegations about the sales to Iranian companies, and it should have known about such sales because information posted on the websites of the SAP resellers publicized their ties to Iranian companies.

Understand regulatory obligations. OFAC found that MoneyGram had an "erroneous misunderstanding of its obligations." There appear to have been two such misunderstandings. One was that, in at least some cases, MoneyGram "improperly determined that the commercial transactions qualified as non-commercial, personal remittances." The second was that it "erroneously believed that [SDN List] screening of inmates in federal prison was not expected under the BOP program." While some of the particular OFAC sanctions programs carve out the official business of the United States from their prohibitions or contain regulatory authorizations for otherwise prohibited conduct when carried out by employees, contractors, or grantees of the United States government, the requirements of US sanctions generally remain in effect in connection with US government work.

Consider implementing IP geolocation screening and blocking. OFAC has repeatedly emphasized in recent cases, such as those involving Bitgo, Inc. and BitPay, Inc., that it expects companies with access to relevant IP information and whose products and services are at risk of being accessed by persons in sanctioned jurisdictions to implement IP screening and blocking controls. For years, SAP failed to implement geolocation IP address screening despite internal audits identifying the vulnerability in its compliance program.

Use effective screening tools. One of the "root causes" of sanctions violations identified in the Framework is outdated or inadequate screening tools. Here, even when MoneyGram began screening transactions involving blocked federal inmates, it continued to process such transactions due to other screening, technology, and fuzzy logic failures. OFAC credited the company for having later undertaken to remedy these errors by retiring its legacy screening system and replacing it with an improved one.

Act on the findings of internal audits and whistleblower reports. As the Framework highlights,

audits are an important element of an effective sanctions compliance program. Importantly, companies should appropriately address the findings of such audits. In calculating the applicable civil monetary penalty in the SAP case, OFAC found an aggravating factor to be that, for years, the company had failed to act on sanctions compliance deficiencies identified in multiple internal audits.

Cooperation with regulators during an investigation may require significant resources. Both MoneyGram and SAP received credit for their cooperation during the investigation. OFAC does not provide details regarding the nature and extent of MoneyGram's cooperation, but SAP's cooperation credit reflected both OFAC's and DOJ's view that the company expended significant time and resources toward what appeared to have been a forward-leaning investigation. SAP cooperated with prosecutors and investigators by producing thousands of translated documents, answering inquiries and, notably, making foreign-based employees available for interviews in a mutually agreed-on overseas location.

Mr. Dawson, Mr. Meltzer, Mr. Horn, Mr. Goldman, Ms. Nikou, and **Ms. Lindblom** are lawyers at Wilmer Cutler Pickering Hale and Dorr LLP. Ranging from partners to associates, the group of lawyers are based out of the international law firm's New York and Washington, DC offices. Combined they have deep experience in counseling clients in the financial services and fintech sectors and with international trade and policy needs. To learn more, visit *www.wilmerhale.com*.

NOTES

1 The eight cases in which OFAC has issued civil penalties this year represent twice the number of such cases through this point in 2020.

2 US Dep't of Treasury, OFAC Settles with SAP SE for Its Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations (Apr. 29, 2021).

3 According to the DOJ press release announcing the NPA, SAP spent more than $27 million to improve its compliance program over the course of four years. Press Release, US Dep't of Justice, SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ (Apr. 29, 2021).

4 Pursuant to the NPA, SAP agreed to disgorge $5.14 million. *See id*.

5 US Dep't of Justice, NPA (Apr. 20, 2021), at para. 1(e).

6 US Dep't of Treasury, OFAC Enters into $34,328.78 Settlement with MoneyGram Payment Systems, Inc. for Apparent Violations of Multiple Sanctions Programs (Apr. 29, 2021).

7 OFAC's enforcement action against MoneyGram appears to be the agency's first public enforcement action involving transactions with US incarcerated blocked individuals.