August 13, 2021

OFAC Enforcement Action against U.S. Payments Company Shows the Importance of Robust Sanctioned Person and Location Screening

On July 23, 2021, the U.S. Department of the Treasury's Office of Assets Control ("OFAC") announced a $1,400,301 settlement agreement with a New York-based online money transmitter and provider of prepaid access, Payoneer Inc. ("Payoneer"), to resolve 2,260 apparent violations of multiple OFAC sanctions programs.[1] OFAC determined that Payoneer's sanctions compliance program—in particular its sanctioned person and location screening procedures—had several deficiencies that allowed persons located in sanctioned jurisdictions and persons on OFAC's Specially Designation Nationals and Blocked Persons List (the "SDN List") to engage in approximately $802,117 worth of transactions via Payoneer's services.

This OFAC enforcement action highlights that money services and payments businesses (like all financial service providers) are responsible for ensuring that they do not engage in unauthorized transactions prohibited by U.S. sanctions and that, therefore, such businesses should develop a tailored, risk-based sanctions compliance program in line with the guidance provided by OFAC in its *Framework for OFAC Compliance Commitments*.[2] This enforcement action also emphasizes the importance of effective screening not only for designated persons (including those persons on the SDN List), but also for persons located in comprehensively sanctioned jurisdictions—including ensuring that shipping or billing address information, IP addresses, or business identifier codes (BICs) collected in the normal course of a company's business are screened. Additionally, this action is a reminder of the need to periodically test and audit sanctions screening procedures and systems to ensure that they are flagging transactions accurately and otherwise operating effectively.

Below we provide more detail on OFAC's enforcement action and its implications.

The Apparent Violations

According to OFAC, between February 4, 2013 and February 20, 2018, Payoneer processed 2,260 transactions totaling $802,117 in apparent violation of multiple OFAC sanctions programs. OFAC noted that, although Payoneer's policies and procedures dating back to as far as June 2015 had specified that transactions involving sanctioned persons or persons located in sanctioned jurisdictions were prohibited, the testing and auditing that Payoneer had conducted to verify that these policies and procedures were being implemented failed to identify several compliance deficiencies that led to the apparent violations.

---

1 OFAC, "OFAC Enters Into $1,400,301.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Programs," (Jul. 23, 2021), available here (the "OFAC Web Notice").

2 *See* OFAC, "A Framework for OFAC Compliance Commitments," (May 2, 2019), available here.

OFAC stated that the apparent violations related to commercial transactions processed by Payoneer on behalf of its corporate customers and card-issuing financial institutions. According to OFAC, these apparent violations resulted from multiple sanctions compliance control breakdowns at Payoneer, including: "(i) weak algorithms that allowed close matches to SDN List entries not to be flagged by its filter, (ii) failure to screen for Business Identifier Codes (BICs) even when SDN List entries contained them, (iii) during backlog periods, allowing flagged and pended payments to be automatically released without review, and (iv) lack of focus on sanctioned locations, especially Crimea, because [Payoneer] was not monitoring IP addresses or flagging addresses in sanctioned locations."[3]

OFAC determined that Payoneer's processing of these 2,260 transactions resulted in apparent violations of multiple sanctions programs, including the Crimea, Zimbabwe, Weapons of Mass Destruction Proliferators, Iran, Sudan, and Syria sanctions programs.

Factors Affecting OFAC's Penalty Determination

OFAC indicated that Payoneer voluntarily self-disclosed 19 of the transactions, while the remaining 2,241 transactions were not voluntarily self-disclosed. OFAC went on to state that all of the transactions were non-egregious violations. According to OFAC, the statutory maximum civil monetary penalty amount for the apparent violations was $666,142,614 and the base penalty amount was $3,889,726.

OFAC noted as aggravating factors that Payoneer "failed to exercise a minimal degree of caution or care for its sanctions compliance obligations when it allowed persons on the SDN List and persons in sanctioned locations to open accounts and transact as a result of deficient sanctions compliance processes that persisted for a number of years."[4] OFAC also noted as an aggravating factor that Payoneer had a "reason to know the location of the users it subsequently identified as located in jurisdictions and regions subject to sanctions based on common indicators of location within its possession, including billing, shipping, or IP addresses, or copies of identification issued in jurisdictions and regions subject to sanctions."[5] OFAC also faulted Payoneer for causing harm to six different OFAC sanctions programs.

OFAC noted several mitigating factors including that upon discovering the apparent violations, Payoneer's "senior management acted quickly to self-disclose the [a]pparent [v]iolations related to blocked persons and provided substantial cooperation throughout the investigation."[6] OFAC also praised Payoneer for taking a number of remedial measures, including the following:

- "Replacing [Payoneer's] Chief Compliance Officer, retraining all compliance employees, and hiring new compliance positions focused specifically on testing;"
- "Enhancing its screening software to include financial institution alias names and BIC codes and automatically triggering a manual review of payments or accounts that match persons on the SDN List;"
- "Enabling the screening of names, shipping and billing addresses, and IP information associated with account holders to identify jurisdictions and regions subject to sanctions;"
- Instituting holds on pending transactions flagged for review "instead of allowing them to complete during a backlog; and"

[3] OFAC Web Notice at 1.

[4] OFAC Web Notice at 2.

[5] *Id*.

[6] *Id*.

- "A daily review of identification documents uploaded to Payoneer, and a rule engine that stops payments with identification indicating jurisdictions and regions subject to sanctions."[7]

Implications

The Payoneer settlement agreement is one of several recent OFAC enforcement actions involving sanctions screening deficiencies. These settlements show the importance of not only implementing sanctions screening procedures, but also of testing and auditing the implementation of those procedures to ensure that they are working in practice to identify potentially problematic transactions.

Importantly, as the Payoneer action shows, OFAC not only expects that companies will screen customers' and counterparties' names against lists of sanctioned persons, including the SDN List, but also that companies will perform screening of other information about customers and counterparties that companies receive during the normal course of their business, including information that would make a company aware of the jurisdiction in which their customer or counterparty is located. For example, in this settlement OFAC specifically faulted Payoneer for its failure to screen "common indicators of location within its possession, including billing, shipping, or IP addresses, or copies of identification issued in jurisdictions and regions subject to sanctions."

The settlement also shows the importance of incorporating unique identifiers (such as, in this action, BIC codes) that are provided in SDN List or other sanctions list entries into companies' sanctions screening procedures, as these unique identifiers can provide a strong indication of a potential true "hit" against an OFAC sanctions list. While not discussed in this action including place names associated with sanctioned jurisdictions—such as, depending on the jurisdiction, the names of cities, regions, ports, and common alternative spellings of the same—in a sanctions filter can be a useful means of further detecting the potential involvement of a sanctioned jurisdiction.[8]

The Payoneer settlement is also one of several recent OFAC enforcement actions to focus on the lack of IP address screening by companies engaged in online business. These recent enforcement actions have made clear that OFAC expects companies doing business online to screen the IP address information that they receive in the normal course of their business and to implement IP blocking where possible. Financial sector entities with significant international business that lack the resources or skill set to develop a robust internal screening system may wish to consider obtaining the support of a reputable sanctions screening vendor.

The settlement also shows the importance of having "hard" holds in place with regard to transactions that are flagged via a company's sanctions screening procedure. OFAC specifically faulted Payoneer for having a sanctions screening process that automatically cleared flagged transactions during periods of "backlog" within the sanctions screening system. It is clear from the Payoneer settlement that OFAC expects companies to perform a review of all transactions flagged for sanctions-related reasons before clearing them to proceed.

We will continue to monitor enforcement actions taken by OFAC and provide further updates as appropriate.

* * *

[7] OFAC Web Notice at 3.

[8] *See* OFAC, "OFAC Settles with Amazon.com, Inc. with Respect to Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs," (Jul. 8, 2020), available here (OFAC faulted a screening filter that did not flag transactions involving, among other things, cities in Crimea or alternate spellings of Crimea such as "Krimea").

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:

Jessica S. Carey
+1-212-373-3566
jcarey@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 Fiorill
+1-202-223-7346
rfiorill@paulweiss.com

Associate Joshua R. Thompson contributed to this memorandum.