Guidepost

PAYONEER OFAC SETTLEMENT PROVIDES DIRECTION FOR FINTECH COMPLIANCE OFFICERS

The regulatory landscape for fintechs is continually evolving. It is critical that compliance officers stay on top of what is going on in the industry to ensure they make the best decisions and take proactive measures in alignment with current regulations. The recent OFAC settlement with Payoneer, Inc. for apparent violations of multiple sanctions programs is an excellent case study for compliance officers with fintechs and payment processors to heed when enhancing their compliance programs.

For those not familiar with the matter, Payoneer paid a more than $1.4 million monetary penalty to settle the action to cover 2,260 apparent violations — 2,241 payments were made to parties in jurisdictions subject to sanctions and 19 payments were made on behalf of Sanctioned Designed Nationals ("SDNs").

The four-page enforcement order release offers several key lessons:

Compliance control breakdowns at Payoneer included:

1. weak algorithms that allowed close matches to the SDN list to go unflagged by its filter
2. failure to screen for bank BIC codes even when that information was part of the SDN list entries
3. when backlogs occurred, flagged payments were released without manual review
4. lack of focus on monitoring IP addresses in sanctioned locations

Aggravating factors:

1. the compliance deficiencies persisted for a number of years
2. Payoneer had information in its possession that should have revealed the locations in sanctions jurisdictions (IP addresses, billing addresses,

identification, etc.)

3. violations of six sanctions programs

Mitigating factors:

1. self-disclosure and cooperation
2. no previous penalties in the preceding five years
3. comprehensive remediation efforts including a new CCO, enhanced screening software, screening of IP addresses, billing addresses and other identifying information for account holders, rule enhancements to stop payments with identifying factors in sanctions jurisdictions

Once again, through this settlement, OFAC specifically notes that money service businesses should develop an OFAC compliance program and refers to the OFAC Framework for Compliance Guidance issued in May 2019.

What is particularly noteworthy is that Payoneer had policies in place, but still fell short. What went wrong? The key deficiencies were in screening, testing, auditing and transaction review procedures which goes to prove that even the best compliance procedures need constant testing.

Test, Test, Test

Now is the time to review your organization's OFAC compliance program and procedures. It is imperative that you can confidently answer the following questions:

- Are you regularly testing your sanctions program?
- Have you conducted a sample lookback of transactions or audited your escalation procedures?
- How are your sanctions filters set?
- Are you capturing IP addresses?
- Are you screening for IP addresses?
- What is your policy for customer use of VPNs or other anonymizing tools?
- How do you handle a backlog?

If you can't answer these questions, then take action to get the answers. If you don't have the bandwidth to conduct such testing, engage an outside expert to help. In the long run, testing can help you keep from running afoul of regulations and the potential for costly fines.