October 6, 2022

# OFAC Enforcement Action Again Highlights the Importance of IP Address Blocking; OFAC Also Issues Guidance for Instant Payments Industry

On September 30, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") announced a $116,048 settlement with Tango Card, Inc. ("Tango Card"), a U.S.-headquartered company that supplies and distributes electronic rewards, often in the form of digital stored value cards to support client businesses' employee and customer incentive programs. The settlement resolves 27,720 transactions with persons with an internet protocol ("IP") address or email address associated with Cuba, Iran, Syria, North Korea, and the Crimea region that resulted in apparent violations of U.S. sanctions.[1] OFAC determined that although Tango Card maintained IP blocking and sanctions screening procedures for its direct customers (i.e., merchants), Tango Card did not maintain such procedures with regard to the recipients of rewards (i.e., the merchant's customers and employees) despite collecting information, including such recipients' IP addresses and email addresses, during the normal course of its business.

This enforcement action 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 email address suffixes collected during the normal course of a company's business are screened. This enforcement action thus reinforces several recent OFAC enforcement actions in which OFAC faulted companies in the cryptocurrency space[2] and a payment processor[3] for similar deficiencies in their sanctions screening and IP blocking procedures.

On the same day, OFAC separately issued new guidance entitled *Sanctions Compliance Guidance for Instant Payment Systems* (the "Guidance") that discuss approaches that financial institutions that participate in instant real-time payments systems (and developers of these systems) can take to mitigate their sanctions compliance risks.[4] OFAC stated that it was issuing the Guidance to "(i) reaffirm that financial institutions should take a risk-based approach to managing sanctions risks; (ii) highlight key factors that may be relevant in determining that risk-based approach; (iii) encourage the development and deployment of innovative sanctions compliance approaches and technologies to address identified risks; and (iv) encourage developers of instant payment systems to incorporate sanctions compliance considerations as they develop new payment technologies."[5] The Guidance also noted that OFAC issued the Guidance to assist financial institutions in determining how to best allocate their compliance resources in a risk-based manner.

Below we provide more detail on OFAC's enforcement action and the Guidance.

## The Tango Card Settlement

According to OFAC, between September 2016 and September 2021, Tango Card digitally transmitted 27,720 merchant gift cards and promotional debit cards totaling $386,828 to individuals with email or IP addresses associated with Cuba, Iran, Syria, North Korea, or the Crimea region. OFAC stated that while Tango Card used geolocation tools to identify transactions involving comprehensively sanctioned jurisdictions and countries at high risk for suspected fraud for (and performed sanctions screening of) its direct customers, which were merchants, Tango Card did not use these controls to identify whether recipients of rewards, which were customers and employees of merchants, may involve comprehensively sanctioned jurisdictions, despite collecting relevant information including IP address and top level domains ("TLD"; i.e., email address suffixes associated with comprehensively sanctioned jurisdictions such as .ir (Iran) and .cu (Cuba)) of such recipients in the normal course of its business.

OFAC indicated that Tango Card voluntarily self-disclosed these apparent violations, which the agency determined were non-egregious. According to OFAC, the statutory maximum civil monetary penalty amount for the apparent violations was $9,168,949,062 and the base penalty amount was $193,414.

OFAC noted as aggravating factors that Tango Card "failed to impose risk-based geolocation rules using tools at its disposal to identify the location of its reward recipients, despite having reason to know that it was transmitting rewards to recipients in sanctioned jurisdictions based on IP address and TLD data in its possession."[6]

OFAC noted several mitigating factors, including a number of remedial measures that Tango Card took to enhance its sanctions compliance framework. Among other things, OFAC praised Tango Card for taking the following measures to strengthen its sanctions compliance processes:

- "implement[ing] geo-blocking for TLDs, preventing reward issuance to email addresses associated with sanctioned jurisdictions;
- Update[ing] its IP address geo blocking to include jurisdictions and regions subject to sanctions, preventing redemptions by persons in these jurisdictions;
- Conduct[ing] training for the team that handles bulk spreadsheet orders for manually screening email addresses for jurisdictions and regions subject to sanctions;
- Hir[ing] a consultant to review its security posture with regard to its cloud program;
- Hir[ing] and continu[ing] to hire additional staff to proactively identify control gaps and improve compliance processes;
- Acquir[ing] additional screening tools; and
- Running two monthly reports — one identifying any TLDs over the prior month from jurisdictions and regions subject to sanctions and the other identifying any IP addresses over the prior month associated with such jurisdictions."[7]

The Tango Card settlement agreement is one of several OFAC enforcement actions involving sanctions screening and IP blocking deficiencies in recent years. These recent enforcement actions have made clear that OFAC expects companies doing business online to screen IP address information, as well as other information that they may receive in the normal course of business (including physical address, email address suffix, TLD data, and phone number prefix information) to identify a nexus with comprehensively sanctioned jurisdictions. While not discussed in this action, in other recent enforcement actions OFAC has noted that 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] These recent settlements also 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.

## Instant Payment Systems Guidance

The Guidance does not set out one standardized approach to sanctions compliance for instant payment systems (i.e., payment systems that allow users to send and receive funds almost instantly, at any time of day on any day of the year, and which likely include cryptocurrency payment systems). Rather, the Guidance notes OFAC's expectation that financial institutions will make decisions on whether and how to screen transactions using instant payment systems based on the institutions' assessment of their own risk. OFAC noted, for example, that solely domestic (i.e., wholly in the United States) instant payment systems generally pose lower sanctions-related risks than those involving accounts maintained at non-U.S. banks, as OFAC "expects that U.S. banks, which are subject to stringent U.S. regulatory requirements and supervisory examinations, are already performing risk-based due diligence on their customers at onboarding and at regular intervals thereafter, including screening their customers to identify a potential sanctions nexus." [9]

While OFAC noted that a payment of any amount could result in a violation of U.S. sanctions, OFAC noted that the monitoring of the nature and value of customer payments made through instant payment systems is an important piece of any financial services business' sanctions compliance framework. OFAC noted, for example, that "payments consistent with past customer behavior that a financial institution has previously vetted and cleared for potential sanctions implications generally pose lower sanctions risk than payments that appear inconsistent with a customer's prior history, such as significantly higher value payments or payments made to foreign persons with whom the customer has not previously dealt." [10]

In the Guidance, OFAC goes on to describe new tools and technologies that financial institutions could use to mitigate their sanctions risks with respect to instant payment systems. These include artificial intelligence tools that leverage information sharing mechanisms across financial institutions that can enhance the accuracy of sanctions screening and reduce the number of false positives. OFAC encouraged financial institutions to use and implement such tools in a manner consistent with an institution's assessment of its sanctions-related risks.

OFAC also encouraged the developers of instant payment systems to incorporate sanctions compliance during the design and development process. As an example, OFAC noted the importance of instant payment systems enabling communication between the financial institutions involved in processing payments, as such communication is often necessary to gather information related to potential sanctions screening alerts. OFAC also encouraged developers of instant payment systems to also create processes in their systems for exception processing (i.e., allowing a transaction to be removed from the automated process to provide sufficient time for a financial institution to investigate potential sanctions concerns). OFAC noted that while it understands that a key feature of instant payment systems is the near real-time nature of transaction settlement, this commercial feature should not discourage financial institutions from implementing risk-based sanctions compliance controls. Finally, OFAC called on instant payment systems to establish minimum sanctions compliance expectations for its members, including, for example, setting expectations for members regarding customer onboarding and ongoing due diligence or norms for screening transaction parties or details, as appropriate based on risk.

The Guidance makes clear that developers of instant payment systems and financial institutions that participate in instant payment systems (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* as well as the Guidance. The Guidance importantly notes that while OFAC recognizes that a key commercial feature of instant payment systems is their speed, OFAC does not view this commercial consideration as outweighing or excusing the need for implementing risk-based sanctions compliance controls relating to payments through instant payment systems.

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

* * *

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

**David Fein**
+44-20-7367-1608
dfein@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

*Associate Joshua R. Thompson contributed to this memorandum.*

---

1 OFAC, "OFAC Settles with Tango Card, Inc. for $116,048.60 Related to Apparent Violations of Multiple Sanctions Programs," (Sept. 30, 2022), available here (the "OFAC Web Notice").

2 *See* OFAC, "OFAC Enters into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," (Dec. 30, 2020), available here; OFAC, "OFAC Enters into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions," (Feb. 18, 2021), available here. These actions were discussed in our year in review memorandum, available here.

3 *See* Paul, Weiss, "OFAC Enforcement Action against U.S. Payments Company Shows the Importance of Robust Sanctioned Person and Location Screening," (Aug. 13, 2021), available here.

4 OFAC, "Sanctions Compliance Guidance for Instant Payment Systems," (Sept. 30, 2022), available here (the "Guidance").

5 *Id*.

6 OFAC Web Notice at 2.

7 OFAC Web Notice at 2-3.

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 (where OFAC determined a screening filter did not flag transactions involving, among other things, cities in Crimea or alternate spellings of Crimea such as "Krimea").

9 The Guidance at 2.

10 *Id*.