DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: December 13, 2023

OFAC Settles with CoinList Markets LLC for $1,207,830 Related to Apparent Violations of the Ukraine-/Russia-Related Sanctions Regulations

CoinList Markets LLC ("CLM"), a San Francisco, California-based virtual currency exchange, has agreed to pay $1,207,830 to settle its potential civil liability arising from processing 989 transactions on behalf of users ordinarily resident in Crimea between April 2020 and May 2022, in apparent violation of OFAC's Russia/Ukraine sanctions. The settlement amount reflects OFAC determination that CLM's apparent violations were not voluntarily self-disclosed and were non-egregious.

Description of the Apparent Violations

CLM, a money services business founded in 2017, allows users to buy, sell, and otherwise trade in crypto tokens and other crypto assets. CLM acts primarily as an intermediary among its users to buy, sell and convert various cryptocurrencies. To do so, users open an account and digital wallet with CLM, during which they provide certain Know-Your-Customer (KYC) information. Individuals, for example, must provide their country of residence, address, date of birth, phone number, selfie picture, and a photo of government issued identification card. Entities must provide similar information, including incorporation documents, country of incorporation, company address, shareholders with 25 percent or more ownership, and information about the entity's signatories.

During the relevant period, CLM maintained several sanctions compliance measures, including screening new and existing customers against OFAC and other sanctions lists, conducting transactional monitoring, and blockchain analytics tools to identify touchpoints with high-risk jurisdictions and sanctioned wallet addresses. When a user submitted an order to trade in virtual currency, moreover, CLM placed a hold on the user's wallet for the amount requested and reviewed it for suspicious activity. Beginning in February 2021, CLM also instituted controls to deny access to users with IP addresses in sanctioned jurisdictions. By spring 2021, CLM's onboarding protocols also included an automated process through which an application was meant to be immediately rejected if a user presented an identification card from, or provided a physical address in, a comprehensively sanctioned jurisdiction.

However, CLM's screening procedures failed to capture users who represented themselves as resident of a non-embargoed country but who nevertheless provided an address within Crimea. In particular, CLM opened 89 accounts for customers, nearly all of whom had specified "Russia" as their country of residence but all of whom provided addresses in Crimea upon account opening, *e.g.*, by identifying a city in Crimea or providing the term "Crimea." Because "Russia" was provided in the country-of-residence field in these instances, CLM's screening protocols failed to recognize that "Crimea" or a city name in Crimea, provided in another data field, indicated likely residence in Crimea.

In providing financial services to these users between April 19, 2020 and May 7, 2022, CLM engaged in 989 apparent violations of the Ukraine-/Russia-Related Sanctions Regulations (URRSR), 31 C.F.R. § 589.207, totaling $1,252,280 (the "Apparent Violations").

Penalty Calculation and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $327,306,583. OFAC determined that the Apparent Violations were not voluntarily self-disclosed and were non-egregious. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter equals the applicable schedule amount, which in this case is $3,097,000. The settlement amount of $1,207,830 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be **aggravating factors**:

(1) CLM failed to exercise due caution or care for its sanctions compliance obligations when it failed to institute internal controls able to flag accounts whose owners described themselves as resident of Crimea.

(2) CLM knew or had reason to know it was conducting transactions on behalf of persons who were likely to be ordinarily resident in Crimea. Each of the users in question self-reported addresses at account opening specifying a city in Crimea, the word "Crimea," or both.

(3) CLM's processing of transactions on behalf of users in Crimea harmed the integrity of the policy objectives of the URRSR. CLM conferred economic benefits to Crimea by processing 989 transactions totaling $1,252,280 over two years. There is no indication the transactions would have been licensable or involved humanitarian activity.

OFAC determined the following to be **mitigating factors**:

(1) OFAC has not issued a Penalty Notice or Finding of Violation to CLM in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations.

(2) CLM cooperated with OFAC's investigation by responding to questions, providing transaction data, and entering into tolling agreements.

(3) The volume of Apparent Violations represents a very small percentage of the total volume of transactions conducted by CLM annually.

(4) CLM undertook a number of remedial measures, including:

- Updating its filter settings to automatically reject potential users who report a residential address with a Crimean city, even if there is no mention of the Crimea region by name, and regardless of the country of residence provided (*e.g.*, Ukraine or Russia);

- Implementation of IP geo-blocking to detect IP addresses in sanctioned jurisdictions and preventing users from accessing their accounts from those IP addresses;

- Investing in new vendors for review and verification of identity documents and restricted party screening as well as in tools to detect the use of VPNs that can obscure users' location; and

- Enhancing its training program and hiring additional experienced compliance personnel.

In view of the individual facts of this case, including CLM's financial circumstances, $300,000 of the settlement amount will be suspended pending satisfactory completion of CLM's compliance commitments as agreed to by CLM as part of this settlement. Moreover, as partial satisfaction of the settlement amount, CLM has also agreed to invest $300,000 in additional sanctions compliance controls, including with respect to enhanced screening controls and additional compliance staff.

Compliance Considerations

This case, like previous OFAC settlement actions with firms operating in the virtual currency space, highlights the importance of integrating all available KYC and other relevant information into a company's screening process and broader compliance function. As demonstrated in previous cases, certain firms providing virtual currency services have failed to ensure that their screening processes and broader compliance programs adequately incorporate customer information gathered from the onboarding process or through transactional information (such as IP location information). Ensuring that such data is gathered and employed using a risk-based approach is important to mitigate the risk of providing services to persons in sanctioned jurisdictions.

This enforcement action further emphasizes the importance for virtual currency companies and those involved in emerging technologies to incorporate risk-based sanctions compliance into their business functions, especially when the companies seek to offer financial services to a global customer base. OFAC's Sanctions Compliance for the Virtual Currency Industry explains that OFAC strongly encourages a risk-based approach to sanctions compliance. An appropriate compliance program for members of the virtual currency industry will depend on a variety of factors, including the type of business involved, its size and sophistication, products and services offered, customers and counterparties, and geographic locations served. It should be predicated on and incorporate five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. Critically, members of the virtual currency and emerging technologies industries should incorporate sanctions compliance considerations at the development and beta testing stages. Delaying development and implementation of a sanctions compliance program can expose companies to a wide variety of potential sanctions risks.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments (Framework) to provide organizations subject to U.S. jurisdiction, as well as foreign entities

that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at Civil Penalties and Enforcement Information | Office of Foreign Assets Control (treasury.gov).

For more information regarding OFAC regulations, please go to: Home | Office of Foreign Assets Control (treasury.gov).