



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: November 28, 2022

OFAC Settles with Virtual Currency Exchange Kraken for \$362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations

Payward, Inc. d/b/a Kraken (“Kraken”), a Delaware-incorporated virtual currency exchange with operations in the United States and elsewhere, has agreed to pay \$362,158.70 to settle its potential civil liability for apparent violations of the Iranian Transactions and Sanctions Regulations. As part of its settlement with OFAC, Kraken also has agreed to invest an additional \$100,000 in certain sanctions compliance controls. Due to Kraken’s failure to timely implement appropriate geolocation tools, including an automated internet protocol (IP) address blocking system, Kraken exported services to users who appeared to be in Iran when they engaged in virtual currency transactions on Kraken’s platform. The settlement amount reflects OFAC’s determination that Kraken’s apparent violations were non-egregious and voluntarily self-disclosed.

Description of the Apparent Violations

Kraken is a centralized global virtual currency exchange that was founded in 2011 and opened for public trading in 2013. Users of the Kraken platform can buy, sell, or hold cryptocurrencies, as well as trade fiat currency for cryptocurrencies, or exchange one cryptocurrency for another. Kraken maintained an anti-money laundering and sanctions compliance program, which included screening customers at onboarding and daily thereafter, as well as review of IP address information generated at the time of onboarding to prevent users in sanctioned jurisdictions from opening accounts. However, despite these controls, between approximately October 14, 2015 and June 29, 2019, Kraken processed 826 transactions, totaling approximately \$1,680,577.10, on behalf of individuals who appeared to have been located in Iran at the time of the transactions.

Although Kraken maintained controls intended to prevent users from initially opening an account while in a jurisdiction subject to sanctions, at the time of the apparent violations, Kraken did not implement IP address blocking on transactional activity across its platform. According to IP address data, account holders who established their accounts outside of sanctioned jurisdictions appear to have accessed their accounts and transacted on Kraken’s platform from a sanctioned jurisdiction.

As a result of the foregoing, Kraken engaged in 826 apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.204 (the “Apparent Violations”).

After identifying this problem, Kraken implemented automated blocking for IP addresses linked to sanctioned jurisdictions. Kraken also implemented multiple blockchain analytics tools to assist with its sanctions monitoring.

Penalty Calculations and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is \$272,228,964. OFAC determined that Kraken self-disclosed the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), 31 C.F.R. part 501, app. A, the base civil monetary penalty applicable in this matter equals the sum of one-half of the transaction value for each Apparent Violation, which is \$840,288.55.

The settlement amount of \$362,158.70 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. Moreover, Kraken and OFAC have agreed that Kraken will spend an additional \$100,000 to invest in certain additional sanctions compliance controls, including training and technical measures to assist in sanctions screening.

OFAC determined the following to be an **aggravating factor**:

- (1) Kraken failed to exercise due caution or care for its sanctions compliance obligations when, knowing it had customers worldwide, it applied its geolocation controls only at the time of onboarding and not with respect to subsequent transactional activity, despite having reason to know based on available IP address information that transactions appear to have been conducted from Iran.

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

- (1) Kraken has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations.
- (2) Kraken voluntarily self-disclosed the Apparent Violations to OFAC and cooperated with OFAC's investigation into the Apparent Violations.
- (3) Kraken undertook significant remedial measures in response to the Apparent Violations, including the following:
 - adding geolocation blocking to prevent clients in prohibited locations from accessing their accounts on Kraken's website;
 - implementing multiple blockchain analysis tools to assist with sanctions monitoring;
 - investing in additional compliance-related training for its staff, including in blockchain analytics;
 - hiring a dedicated head of sanctions to direct Kraken's sanctions compliance program, in addition to hiring new sanctions compliance staff;

- expanding its contract with its current screening provider to add additional screening capabilities to ensure compliance with OFAC’s “50 Percent Rule,” including detailed reports on beneficial ownership;
- contracting with a vendor that assists with identification and nationality verification by using artificial intelligence tools to detect potential issues with supporting credentials provided by users; and
- implementing an automated control to block accounts using cities and postal codes associated with the Crimea region and in the so-called Donetsk and Luhansk People’s Republics of Ukraine.

Compliance Considerations

As described in OFAC’s [Sanctions Compliance Guidance for the Virtual Currency Industry](#), OFAC strongly encourages a risk-based approach to sanctions compliance. An adequate sanctions 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 also should be predicated on and incorporate at least five essential components: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

Within that framework, this case highlights the importance of using geolocation tools, including IP blocking and other location verification tools, to identify and prevent users located in sanctioned jurisdictions from engaging in prohibited virtual currency-related transactions. In particular, limiting the use of such controls only to the time of account opening — and not throughout the lifetime of the account or with respect to subsequent transactions — could present sanctions risks to virtual currency-related companies. This case also demonstrates the value of a company implementing robust remedial measures after becoming aware of a potential sanctions issue, including the deployment of blockchain analysis tools and compliance-related training on blockchain analytics, as well as committing to future sanctions compliance investments.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published [A Framework for OFAC Compliance Commitments](#) (Framework) in order 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 civil penalties and enforcement information, can be found on OFAC's website at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>.

For more information regarding OFAC regulations, please go to: <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.