DEPARTMENT OF THE TREASURY
OFFICE OF FOREIGN ASSETS CONTROL

OFAC
Office of Foreign Assets Control

Enforcement Release: December 16, 2025

Exodus Movement, Inc. Settles with OFAC for $3,103,360 for Apparent Violations of Iran-related Sanctions Regulations

Exodus Movement, Inc. ("Exodus"), a U.S. financial technology company, has agreed to pay $3,103,360 to settle its potential civil liability for 254 apparent violations of sanctions on Iran administered by the Office of Foreign Assets Control (OFAC). In particular, Exodus provided customer support services to users in Iran which, in certain instances, helped such users access third party digital asset exchanges through Exodus's proprietary wallet software. In some instances, while aware of U.S. sanctions, Exodus staff recommended that these users obscure their location in Iran using Virtual Private Networks (VPNs) to avoid the sanctions compliance controls implemented by such exchanges. The settlement amount reflects the determination by OFAC that the apparent violations were not voluntarily disclosed and that 12 of the 254 apparent violations were egregious, as well as Exodus's extensive remedial efforts and substantial cooperation.

This enforcement action highlights the importance of ensuring that all companies, including new ventures in the financial technology sector, adopt measures to ensure compliance with OFAC sanctions, including by demonstrating strong managerial support, incorporating compliance controls into key business functions, and properly training all relevant personnel.

Description of the Apparent Violations

Exodus's Wallet Product and Customer Service Unit

Exodus is a Delaware-incorporated financial technology company headquartered in Omaha, Nebraska. In July 2016, Exodus began offering free digital asset wallet software called Exodus Wallet as its primary business, which allows users to conduct transactions on various blockchains. Exodus does not store or possess digital assets on behalf of wallet users. Instead, customers use Exodus Wallet to generate and securely store private keys, which can be used to send and receive digital assets in peer-to-peer exchanges or through third party digital asset exchanges. Exodus does not itself process any digital asset exchange transactions, and instead contracts with third-party exchanges to offer their services through Exodus Wallet. During the relevant time period, from about October 2017 to January 2019, Exodus generated revenue by collecting fees each time customers used Exodus Wallet to conduct transactions through such exchanges.

Exodus also maintained a customer support unit to resolve technical issues for users of Exodus Wallet. Exodus generally received customer inquiries via email and provided technical assistance and advice to address issues experienced by its customers, including issues involving Exodus Wallet or access to its exchange partners. Part of Exodus's standard approach to customer support inquiries was to recommend the use of VPNs for privacy and security.

Exodus's Provision of Customer Support Services to Users in Iran

From October 17, 2017 through January 4, 2019, Exodus provided technical and support services on 254 occasions to Exodus Wallet users who identified themselves as located in Iran. This assistance, made in response to user inquiries, generally enabled these users to continue using Exodus Wallet or the services provided by its exchange partners. Exodus staff also regularly recommended the use of VPNs to address technical issues experienced by users in Iran, as it did with other users as well. On several occasions Exodus staff provided customer support services to customers in Iran after the users explicitly asked whether U.S. sanctions on Iran could impact their use of Exodus Wallet.

Exodus provided this customer service support to users in Iran despite the fact that such users' access to Exodus Wallet was prohibited during this time by Exodus's own Terms of Use, which users had to accept before utilizing Exodus Wallet. Among other conditions, the Terms of Use stated that Exodus Wallet and other services and resources available through Exodus "may not be exported or re-exported (a) into any United States embargoed countries, or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals." As a country under comprehensive sanctions, Iran was considered an embargoed country per the Exodus Terms of Use. However, Exodus did not adequately notify or train its employees regarding these sanctions-related prohibitions in the Terms of Use, nor were the Terms of Use accompanied by any other practical mechanism to prevent the use of Exodus Wallet in sanctioned jurisdictions for a significant portion of the relevant time period.

Exodus's Egregious Customer Service Conduct

As noted, Exodus contracts with certain third-party digital asset exchanges, which allows Exodus Wallet users to seamlessly conduct transactions via these exchanges. One such exchange partner—"Exchange A"—announced in April 2018 that it would change its service offerings based on customers' jurisdictions to comply with U.S. regulations. Exchange A then began using Internet Protocol (IP) information to block users in Iran from using its exchange to conduct transactions. As a result of Exchange A's IP blocking of Iran, Exodus customer service staff began receiving an influx of customer service requests from users in Iran who were unable to use Exodus Wallet to conduct transactions via Exchange A.

By May 2018, Exodus became aware that Exchange A blocked users in Iran and understood this may be a measure to comply with U.S. sanctions regulations and other applicable U.S. laws. For example, on May 16, 2018, Exodus's CEO responded to an inquiry about customers in Iran who were unable to access Exchange A by noting that Exchange A was likely blocking such customers to comply with U.S. sanctions regulations. This understanding was shared internally between Exodus management and its customer service staff.

However, Exodus continued to provide customer support services to users located in Iran following Exchange A's blocking of such users. On 12 such occasions, which OFAC determined demonstrated willful and reckless conduct, Exodus customer service staff explained to users in Iran that Exchange A and other exchanges prohibited customers in Iran from using their service due to U.S. sanctions or U.S. laws, generally, but nevertheless recommended the use

of VPNs. The VPN recommendations ultimately enabled such users to continue accessing Exchange A's services via Exodus Wallet by altering the users' IP address and obscuring their location. For example:

- On May 20, 2018, an Exodus customer service representative advised a user identifying themself as located in Iran: "It appears that Iran has been geo-restricted by our exchange partner, [Exchange A] .... From our knowledge previous to this, only Washington and New York state in the USA and North Korea had restrictions. What we learned was this new restriction [is] in place [] due to [Exchange A] following USA law/regulations. I'm terribly sorry to have to relay this news to you, as it came [] as a shock to many of us here at Exodus .... A few of my Iranian customers said that they were able to still use the exchange feature through utilizing a VPN."

- On May 23, 2018, an Exodus customer service representative stated to a user identifying themself as located in Iran: "The reason you're unable to exchange using Exodus is because our exchange partner, [Exchange A], does not allow customers in Iran to exchange with their service, and this extends to Exodus customers as well. This is due to prohibitive regulations, specifically trade sanctions between the USA and Iran." As part of the same customer service interaction, on May 24, 2018, after the same Exodus Wallet user asked a follow-up question about the use of VPNs, another Exodus customer service staff member responded: "When you create an exchange with Exodus, it just forwards your current IP address to [Exchange A]. I expect that [Exchange A] will not be able to detect you are from Iran if you use a VPN to change your IP address."

On 12 occasions, Exodus customer service staff were at least generally aware of applicable U.S. sanctions or U.S. laws in place to restrict users in Iran from engaging with, and conducting transactions through, Exodus's exchange partners, including Exchange A. Despite this awareness, Exodus customer service staff recommended steps to help users access services offered by Exodus's exchange partners, resulting in the circumvention of the control measures employed by the exchanges to block users located in Iran. OFAC has determined that the provision of customer service support on these 12 occasions was egregious.

From about October 2017 to December 2018, Exodus failed to employ an effective compliance program to screen such users for sanctioned jurisdictions, and Exodus lacked policies and controls to prevent Exodus staff from providing them with customer support. This failure was despite the fact Exodus's own Terms of Use prohibited persons in embargoed countries from using Exodus Wallet, conditions that Exodus required users to accept (via self-certification) before using Exodus Wallet. Reflecting its broader lack of a compliance program, Exodus did not notify or train its employees regarding the sanctions-related prohibitions in the Terms of Use and did not provide any other meaningful mechanism to prevent the use of Exodus Wallet in sanctioned jurisdictions.

Accordingly, Exodus's provision of customer support services to persons located in Iran on 254 occasions appears to have violated §560.204 of the ITSR ("Apparent Violations"). Additionally, in 12 egregious instances, the provision of customer support services to customers in Iran also

evaded or avoided, had the purpose of evading or avoiding, caused a violation of, or attempted to violate prohibitions set forth in the ITSR, pursuant to 31 C.F.R. § 560.203.

Penalty Calculations and General Factors Analysis

Under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, Appendix A ("Enforcement Guidelines"), OFAC determined that the apparent violations were not voluntarily disclosed and that 12 of the 254 apparent violations were egregious. Accordingly, under the Enforcement Guidelines, the base civil monetary penalty amount for the 12 egregious Apparent Violations equals the sum of the statutory maximum civil monetary penalty amount for each, which in this case totals $4,532,400. Additionally, the base civil monetary penalty amount for the 242 non-egregious Apparent Violations equals the sum of the applicable schedule amount for each, which in this case totals $242,000. Accordingly, the total base civil monetary penalty amount is $4,774,400.

The settlement amount of $3,103,360 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. OFAC's settlement agreement with Exodus can be found here.

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

(1) On at least 12 occasions, Exodus staff appeared to willfully violate OFAC sanctions on Iran in acknowledging that Exodus's exchange partners prohibited Iranian users from accessing exchange services while recommending the customers use VPNs to circumvent the exchanges' compliance controls. Such conduct, in conjunction with Exodus's broader awareness of U.S. sanctions on Iran, indicates Exodus's knowledge that such conduct constituted or likely constituted a violation of U.S. sanctions.

(2) In other instances, Exodus acted with reckless disregard for U.S. sanctions requirements when it provided customer support services to persons located in Iran on 254 occasions while being generally aware of prohibitions on providing services to Iran, as reflected in its Terms of Use and its CEO's communication to customer support personnel. In doing so, Exodus ignored numerous warning signs that its conduct was prohibited.

(3) Exodus management and staff had actual knowledge that Exodus provided customer support services to users in Iran given that such users generally identified their location in Iran to Exodus staff.

(4) Exodus's conduct was contrary to longstanding U.S. policy directed at denying Iran access to the U.S. and international financial system, including digital assets. These services enabled persons in a comprehensively sanctioned jurisdiction to conduct digital asset transactions using U.S. services and informed them how to obscure their location in Iran, undermining blocking controls implemented by Exodus's exchange partners seeking to comply with U.S. law.

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

(1) Exodus invested millions of dollars in enhancing its sanctions compliance program and took other remedial actions in response to the Apparent Violations. These efforts have included adopting a standalone Export Control and Sanctions Compliance Policy, hiring additional compliance personnel, improving internal compliance policies and procedures, implementing third-party automated sanctions screening and other wallet address monitoring tools, and implementing mandatory sanctions compliance training for all Exodus staff. Exodus also updated the sanctions compliance representations and warranties in agreements with third-party exchange providers and implemented technical measures to prevent dealings with sanctioned cryptocurrency addresses.

(2) Exodus provided substantial cooperation to OFAC over a yearslong investigation, including by responding promptly to OFAC's requests for information, providing large volumes of data regarding the Apparent Violations, participating in witness interviews, submitting internal communications, and executing statute of limitations tolling agreements.

(3) Exodus has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the transactions giving rise to the Apparent Violations. Exodus was also a small company at the time of the Apparent Violations. The volume of the Apparent Violations represents a fraction of a percent of the total number of downloads of the Exodus Wallet and customer support inquiries annually during the relevant time period.

In view of the individual facts of this case, as partial satisfaction of the settlement amount Exodus has agreed to invest $630,000 in additional sanctions compliance controls.

Compliance Considerations

This enforcement action emphasizes the importance of new companies incorporating sanctions compliance into their business functions and providing adequate employee training from day one of operations. This is especially crucial when the companies provide access to financial services to a global customer base. As part of these controls, companies should screen for location information, especially when available through IP addresses and information provided by customers (such as passports or when a customer self-identifies as being from a particular country). Such screening is particularly important in mitigating the risk of providing services to individuals in jurisdictions subject to sanctions.

More broadly, this action highlights that digital asset technology companies—like all financial service providers—are responsible for ensuring that they do not engage in conduct unauthorized by OFAC sanctions. To mitigate such risks, digital asset companies should develop a tailored, risk-based sanctions compliance program. OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry notes that OFAC strongly encourages a customized risk-based approach to sanctions compliance because there is no single compliance program or solution suitable to every circumstance or business. An adequate compliance solution for members of the

digital asset 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, but should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

This action also highlights the significance of management commitment to a sound compliance program. By internally acknowledging that a separate company was bound by sanctions regarding the transactions at issue without addressing the applicability of sanctions to Exodus's business, management failed to prevent these apparent violations.

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 Enforcement Guidelines. These references, as well as recent civil penalties and enforcement information, can be found on OFAC's website at https://ofac.treasury.gov/civil-penalties-and-enforcement-information.

Whistleblower Program

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) maintains a whistleblower incentive program for violations of OFAC-administered sanctions, in addition to violations of the Bank Secrecy Act. Individuals located in the United States or abroad who provide information may be eligible for awards, if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000. FinCEN is currently accepting whistleblower tips.

For more information regarding OFAC regulations, please go to: https://ofac.treasury.gov.