DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Enforcement Release: December 30, 2020

OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

BitGo, Inc. ("BitGo"), a technology company based in Palo Alto, California, that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services, has agreed to remit $98,830 to settle its potential civil liability for 183 apparent violations of multiple sanctions programs (the "Apparent Violations"). As a result of deficiencies related to BitGo's sanctions compliance procedures, BitGo failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its non-custodial secure digital wallet management service. BitGo had reason to know that these users were located in sanctioned jurisdictions based on Internet Protocol (IP) address data associated with devices used to log in to the BitGo platform. At the time of the transactions, however, BitGo failed to implement controls designed to prevent such users from accessing its services. OFAC determined that BitGo did not voluntarily self-disclose the Apparent Violations and that the Apparent Violations constitute a non-egregious case.

This action emphasizes that OFAC sanctions compliance obligations apply to all U.S. persons, including those involved in providing digital currency services. As part of a risk-based approach, OFAC encourages companies that provide digital currency services to implement sanctions compliance controls commensurate with their risk profile.

Description of the Apparent Violations and the Conduct Leading to the Apparent Violations

Between approximately March 10, 2015 and December 11, 2019, BitGo processed 183 digital currency transactions, totaling $9,127.79, on behalf of individuals who, based on their IP addresses, were located in sanctioned jurisdictions. The Apparent Violations related to BitGo's "hot wallet" secure digital wallet management service.[1] Individuals located in Crimea, Cuba, Iran, Sudan, and Syria signed up for "hot wallet" accounts and accessed BitGo's online platform to conduct digital currency transactions.

At the time of the Apparent Violations, BitGo tracked its users' IP addresses for security purposes related to account logins. BitGo, however, did not use this IP address information for sanctions compliance purposes. As a result, users located in Crimea, Cuba, Iran, Sudan, and Syria were able to create and use digital currency wallets on BitGo's platform and engage in digital currency transactions, despite BitGo's ability to identify the location of these users.

Prior to April 2018, BitGo allowed individual users of its secure wallet management services to open an account by providing only a name and email address. In April 2018, BitGo amended its practices to require all new accountholders to also verify the country in which they are located, but BitGo generally relied on each user's attestation regarding their location and did not perform additional verification or diligence on the location of its users. However, after learning of the Apparent Violations, in January 2020, BitGo implemented an OFAC Sanctions Compliance Policy ("OFAC Policy") and undertook significant remedial measures, as further described below.

By failing to prevent users located in Crimea, Cuba, Iran, Sudan, and Syria to access and use its services to engage in digital currency transactions, BitGo apparently violated Executive Order 13685 of

[1] BitGo's "hot wallet" service is a non-custodial service to an online wallet that stores keys online and can be used to send digital currency to other wallets via a public blockchain. The Apparent Violations relate to "hot wallet" services provided by BitGo, Inc. and do not relate to enterprise or custodial services provided by BitGo Inc.'s affiliate, BitGo Trust Company, Inc.

December 19, 2014, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine", the Cuban Assets Control Regulations, 31 C.F.R. §515.201; the Iranian Transactions and Sanctions Regulations, 31 C.F.R. §560.204; the Sudanese Sanctions Regulations, 31 C.F.R. §538.205 (SSR)[2]; and the Syrian Sanctions Regulations, 31 C.F.R. §542.207.

Penalty Calculation and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $53,051,675. OFAC determined that BitGo did not voluntarily self-disclose the Apparent Violations and that the Apparent Violations constitute a non-egregious case. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter is $183,000. The settlement amount of $93,830 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

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

(1) BitGo failed to exercise due caution or care for its sanctions compliance obligations when it failed to prevent persons apparently located in sanctioned jurisdictions to open accounts and send digital currencies via its platform as a result of a failure to implement appropriate, risk-based sanctions compliance controls; and

(2) BitGo had reason to know that some of its users were located in sanctioned jurisdictions based on those users' IP address data, which it had separately obtained for security purposes.

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

(1) BitGo is a relatively small company and has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the apparent violations;

(2) BitGo cooperated with OFAC's investigation into these apparent violations; and

(3) BitGo represented that it has invested in significant remedial measures in response to the Apparent Violations and as part of its agreement with OFAC to implement compliance commitments intended to minimize the risk of recurrence of similar conduct in the future, including:

- BitGo hired a Chief Compliance Officer and implemented its new OFAC Policy, which now applies to all BitGo's services;

[2] Effective October 12, 2017, pursuant to Executive Order 13761 (as amended by Executive Order 13804), U.S. persons are no longer prohibited from engaging in transactions that were previously prohibited solely under the SSR. Consistent with the revocation of these sanctions, OFAC removed the SSR from the Code of Federal Regulations on June 29, 2018. However, the revocation of these sanctions does not affect past, present, or future OFAC enforcement investigations or actions related to any apparent violations of the SSR arising from activities that occurred prior to October 12, 2017.

- BitGo implemented a new OFAC Policy that includes:
    - A detailed overview of OFAC and relevant sanctions laws;
    - The appointment of a compliance officer specifically responsible for implementing and providing guidance and interpretation on matters related to U.S. sanctions laws;
    - IP address blocking, as well as email-related restrictions, for sanctioned jurisdictions;
    - Periodic batch screening;
    - Recordkeeping procedures for all financial records and documentation related to sanctions compliance efforts;
    - A review and, where appropriate, update of end-user agreements to ensure that customers are aware of, and comply with, U.S. sanctions requirements; and
    - A review of screening configuration criteria on a periodic basis.
- BitGo screens all accounts, including "hot wallet" accounts, against OFAC's Specially Designated Nationals and Blocked Persons List, including blocked cryptocurrency wallet addresses identified by OFAC. BitGo has also conducted a retroactive batch screen of all users;
- BitGo routinely reviews its OFAC Policy and updates its procedures, as appropriate; and
- BitGo employees are required to certify that they have reviewed and understand BitGo's OFAC Policy, and are required to attend training programs, as appropriate.

Compliance Considerations

This action highlights that companies involved in providing digital currency services—like all financial service providers—should understand the sanctions risks associated with providing digital currency services and should take steps necessary to mitigate those risks. Companies that facilitate or engage in online commerce or process transactions using digital currency are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions.

To mitigate such risks, administrators, exchangers, and users of digital currencies should develop a tailored, risk-based sanctions compliance program. OFAC's *A Framework for OFAC Compliance Commitments* notes that each risk-based sanctions compliance program will vary depending on a variety of factors, including the company's size and sophistication, products and services, customers and counterparties, and geographic locations, 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. Within that framework, this enforcement action emphasizes the importance of implementing technical controls, such as sanctions list screening and IP blocking mechanisms, to mitigate sanctions risks in connection with digital currency services.

Additional guidance from OFAC related to the provision of digital currency services can be found here: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published *A Framework for OFAC Compliance Commitments* 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 U.S.-origin goods or services, 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 is discussed in OFAC regulations governing the various sanctions programs and in 31 C.F.R. Part 501. On November 9, 2009, OFAC published as Appendix A to Part 501 the Economic Sanctions Enforcement Guidelines. *See* 74 Fed. Reg. 57,593 (Nov. 9, 2009). The Economic Sanctions Enforcement Guidelines, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at http://www.treasury.gov/ofac/enforcement.

For more information regarding OFAC regulations, please visit: http://www.treasury.gov/ofac.