

SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY



Office of Foreign Assets Control

October 2021





OFAC

Office of Foreign Assets Control

CONTENTS

Introduction	1	Sanctions Compliance Best Practices for the Virtual Currency Industry	10
What Is OFAC?	2	Management Commitment	11
What Are OFAC Sanctions?	3	Risk Assessment	12
The SDN List	4	Case Study: Diagnosing Risky Relationships.....	12
How Do You Block Virtual Currency?.....	5	Internal Controls.....	13
Case Study: OFAC Sanctions Involving Virtual Currency	5	Case Study: Double-Duty Data.....	13
Who Must Comply with OFAC Sanctions?.....	6	Sanctions Screening	16
Strict Liability Regulations	6	Remediating the Root Causes of Violations.....	17
OFAC Requirements and Procedures.....	7	Risk Indicators.....	17
Reporting Requirements.....	7	Testing and Auditing	18
Recordkeeping Requirements.....	8	Training	19
License Procedures.....	8	OFAC Resources.....	20
Consequences of Noncompliance	9	FAQs on Virtual Currency Topics.....	20
Enforcement Procedures.....	9	Contact Information.....	21
Enforcement Guidelines.....	9	Resource Sites	22
Enforcement Actions.....	9		
Voluntary Self-Disclosure.....	9		



INTRODUCTION

Virtual currencies are beginning to play an increasingly prominent role in the global economy. The growing prevalence of virtual currency as a payment method likewise brings greater exposure to sanctions risks—like the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction. Accordingly, the virtual currency industry, including technology companies, exchangers, administrators, miners, wallet providers, and users, plays an increasingly critical role in preventing sanctioned persons from exploiting virtual currencies to evade sanctions and undermine U.S. foreign policy and national security interests. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this guidance to assist the virtual currency industry in mitigating these risks.

OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies. Members of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related transactions. This guidance will assist those in the virtual currency industry in:

 **Evaluating sanctions-related risks in their lines of business**

 **Building a risk-based sanctions compliance program**

 **Protecting their business from sanctions violations and intentional misuse of virtual currencies by malicious actors**

 **Understanding OFAC's recordkeeping, reporting, licensing, and enforcement processes**

OFAC is committed to engaging with the virtual currency industry to promote understanding of, and compliance with, sanctions requirements and due diligence best practices.

VIRTUAL CURRENCY VS DIGITAL CURRENCY

What do these terms mean for purposes of OFAC sanctions?

Digital Currency includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency



Virtual Currency is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and is neither issued nor guaranteed by any jurisdiction.

What is OFAC?

The Office of Foreign Assets Control (OFAC) is the office within the U.S. Department of the Treasury that is responsible for administering and enforcing economic sanctions against targeted foreign countries, geographic regions, entities, and individuals to further U.S. foreign policy and national security goals. Economic sanctions are used by the U.S. government to prevent targets such as terrorists, international narcotics traffickers, weapons of mass destruction proliferators, and perpetrators of serious human rights abuse from accessing the U.S. financial system for purposes contrary to U.S. foreign policy and national security interests, and to change the behavior of such targets. In this way, among others, economic sanctions can be a powerful foreign policy tool, but the effectiveness of sanctions relies upon the active participation of everyone subject to U.S. jurisdiction, including those within the virtual currency industry.

What are OFAC Sanctions?

OFAC administers over 35 different sanctions programs—each designed to respond to specific threats and to further U.S. foreign policy and national security goals. As a result, the types of sanctions employed in each program may differ. Generally, OFAC sanctions can be either comprehensive or targeted in nature and can require the blocking of assets or impose restrictions on financial or trade-related activities with a specific person, country, region, or government.

The most comprehensive sanctions programs that OFAC administers typically include several or all of the following types of sanctions, while other sanctions programs may only employ some of these options:



Broad trade-based sanctions or embargoes

prohibit dealings with an entire country or geographic region, unless exempt or authorized. This type of sanction usually includes a prohibition on importing or exporting goods or services to or from the sanctioned jurisdiction. Such sanctioned jurisdictions currently include Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine.



Government or regime sanctions

either (1) require the blocking of all property and interests in property of a particular foreign government or regime that are or come within the United States or the possession or control of a U.S. person, or (2) prohibit specific types of transactions and activities involving a particular foreign government or regime.



List-based sanctions

target specific, listed individuals and entities and either (1) require the blocking of all property and interests in property of those listed persons that are or come within the United States or the possession or control of a U.S. person, or (2) prohibit specific types of transactions and activities with listed persons.



Sectoral sanctions

target individuals and entities operating in specific sectors of a foreign country's economy or prohibit specific activities associated with a sector of a foreign country's economy.

In its administration of list-based sanctions, OFAC maintains several public lists of individuals and entities and their identified blocked property, such as aircraft and vessels, targeted by OFAC sanctions. The most prominent among these is the Specially Designated Nationals



and Blocked Persons List, known as the “SDN List.” Both the SDN List and the Consolidated Sanctions List — a list that combines all other sanctions lists maintained by OFAC — are available for public use in a number of different [data formats and data schemas](#). To make it easier to screen and use OFAC’s sanctions lists for compliance purposes, OFAC has a free search tool, the [Sanctions List Search](#), which can conduct searches across all of the sanctions lists administered by OFAC.

As explained in OFAC’s 50 Percent Rule, OFAC’s sanctions lists do not separately list the names of all entities owned 50 percent or more by blocked persons, or the countries, regions, or governments subject to more comprehensive sanctions. OFAC’s sanctions programs are dynamic, so prior due diligence on the parties and locations with which you plan to do business is essential. For more program-specific sanctions information, please visit OFAC’s [Sanctions Programs and Country Information webpage](#).

The SDN List

OFAC’s Specially Designated Nationals and Blocked Persons List (the “SDN List”) is one of the lists of sanctioned persons that OFAC publishes as part of its enforcement efforts.* The SDN List includes certain individuals and entities sanctioned due to their nexus to a targeted country, geographic region, or regime. The SDN List also includes individuals, groups, and entities, such as terrorists, narcotics traffickers, and human rights abusers designated under sanctions programs that are not jurisdiction specific. Collectively, designated individuals and entities are called “Specially Designated Nationals and blocked persons” or “SDNs.” As of the date of publication, OFAC’s SDN List contains over 9,000 names (or variations thereof) of designated individuals and entities located around the world, as well as identifications of certain property blocked by sanctions such as vessels and aircraft. The SDN List is frequently updated, and you can [sign up](#) to receive email notifications whenever OFAC updates its SDN List.

Additionally, pursuant to OFAC’s “50 Percent Rule,” any entity owned, directly or indirectly, 50 percent or more, individually or in the aggregate by one or more blocked persons, is also considered a blocked person even if that entity does not itself appear on the SDN List—and the same restrictions apply. (See [Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked](#), August 13, 2014.)

In general, unless exempt or authorized by OFAC, U.S. persons are prohibited from engaging in transactions with SDNs or blocked persons, directly or indirectly, and must block any property in their possession or control in which an SDN or a blocked person has an interest.

*To learn more about other sanctions lists maintained by OFAC, visit OFAC’s [“Other OFAC Sanctions Lists”](#) webpage.

How Do You “Block” Virtual Currency?

Once a U.S. person determines that they hold virtual currency that is required to be blocked pursuant to OFAC’s regulations, the U.S. person *must deny all parties access* to that virtual currency, ensure that they comply with OFAC regulations related to the holding and reporting of blocked assets, and implement controls that align with a risk-based approach. U.S. persons are not obligated to convert the blocked virtual currency into traditional fiat currency (e.g., U.S. dollars) and are not required to hold such blocked property in an interest-bearing account. Blocked virtual currency *must be reported to OFAC within 10 business days*, and thereafter on an annual basis, so long as the virtual currency remains blocked. (See [OFAC Frequently Asked Question \(FAQ\) 646](#).)



CASE STUDY

OFAC Sanctions Involving Virtual Currency

In recent years, OFAC sanctions have increasingly targeted individuals and entities that have used virtual currency in connection with malign activity. For example, on [March 2, 2020](#), OFAC sanctioned two Chinese nationals involved in a North Korean state-sponsored money-laundering scheme. The individuals received approximately \$100 million in virtual currency stolen from cyber intrusions against two virtual currency exchanges and began layering the funds in complex transactions to include purchasing over \$1 million in digital music gift cards. More recently, on [September 21, 2021](#), OFAC designated a Russian virtual currency exchange for facilitating financial transactions for ransomware actors. Based on analysis of known transactions, over 40 percent of the exchange’s transaction history had been associated with illicit actors, involving the proceeds from at least eight ransomware variants. As sanctioned persons and countries become more desperate for access to the U.S. financial system, it is vital that the virtual currency industry prioritize cybersecurity and implement effective sanctions compliance controls to mitigate the risk of sanctioned persons and other actors exploiting virtual currencies to undermine U.S. foreign policy interests and national security.

Who Must Comply with OFAC Sanctions?

All U.S. persons are required to comply with OFAC regulations. This includes all U.S. citizens and lawful permanent residents, wherever located; all individuals and entities within the United States; and all entities organized under the laws of the United States or any jurisdiction within the United States, including any foreign branches of those entities. Accordingly, anyone engaging in virtual currency activities in the United States, or that involve U.S. individuals or entities, should be aware of OFAC sanctions requirements and the circumstances in which they must comply with those requirements.

Depending on the authorities governing each sanctions program, others may also be required to adhere to OFAC sanctions requirements. For example, OFAC's Cuba, Iran, and North Korea sanctions programs extend sanctions prohibitions to certain foreign entities owned or controlled by U.S. persons or U.S. financial institutions. Certain activities by non-U.S. persons that involve the United States, U.S. persons, or goods or services exported from the United States may also be subject to OFAC sanctions regulations.

Additionally, in most sanctions programs, any transaction that causes a violation — including a transaction by a non-U.S. person that causes a U.S. person to violate sanctions — is also prohibited. For certain sanctions programs, U.S. persons, wherever located, also are prohibited from facilitating actions on behalf of non-U.S. persons if the activity would be prohibited by sanctions regulations if directly performed by a U.S. person or within the United States.

Strict Liability Regulations

OFAC may impose civil penalties for sanctions violations generally based on a strict liability legal standard. This means that, in many cases, a U.S. person may be held civilly liable for sanctions violations even without having knowledge or reason to know it was engaging in such a violation. As a general matter, however, OFAC takes into consideration the totality of facts and circumstances surrounding an apparent violation to determine the appropriate enforcement response. For example, OFAC may consider as mitigating factors a virtual currency company's implementation of a risk-based OFAC compliance program and remedial measures taken in response to an apparent violation. For more information, see section III of the [Enforcement Guidelines, General Factors Affecting Administrative Action](#).

OFAC Requirements and Procedures

Several OFAC requirements and procedures, such as certain reporting and recordkeeping requirements and licensing procedures, uniformly apply across sanctions programs. For a more complete description of these requirements and procedures, refer to 31 C.F.R. Part 501, [Reporting, Procedures and Penalties Regulation \(RPPR\)](#), and OFAC's answers to [frequently asked questions \(FAQs\) on reporting requirements](#).

Reporting Requirements

 *Initial Blocked Property Reports* must be filed within 10 business days following the date that property is blocked.

 *Annual Blocked Property Reports* on all blocked property held as of June 30 of the current year must be filed annually no later than September 30 of each year.

 *Rejected Transaction Reports* must be filed within 10 business days of the date the transaction was rejected due to sanctions requirements.

 *On Demand Reports* of information related to transactions or property subject to OFAC's regulations may be required by OFAC at any time, through an administrative subpoena. (See 31 C.F.R. § 501.602 for more information.)

OFAC strongly encourages filers to submit initial blocked property and rejected transaction reports through OFAC's secure electronic reporting platform, the [OFAC Reporting System \(ORS\)](#). To register to submit such reports through ORS, or for ORS program information, please email ofacreport@treasury.gov.

Recordkeeping Requirements

 *Who?* Every person engaging in transactions subject to OFAC's regulations, and holders of blocked property, must keep records and make those records available for examination.

 *What?* Full and accurate records are required for each transaction subject to OFAC's regulations, including transactions processed pursuant to a license (whether a general license or a specific license), and of blocked property held.

 *How long?* Required records must be maintained for five years after the date of the transaction or, with respect to blocked property, five years after property is unblocked.

License Procedures

OFAC may make exceptions to permit activity prohibited by sanctions or not otherwise exempt. These exceptions may take the form of *general licenses*, which are publicly issued, self-executing authorizations that permit performance of certain categories of transactions or activities by all U.S. persons, or by persons identified in the relevant sanctions authorities.

Upon request, OFAC also may issue *specific licenses*, which are authorizations issued in response to a specific license application that allow the applicant to engage in specific transactions or activities that otherwise would be prohibited, or individualized *interpretive guidance*, if appropriate, to help clarify how regulatory requirements apply to a specific transaction. Each request for a specific license or interpretive guidance is reviewed by OFAC on a case-by-case basis and often requires coordination with other U.S. government agencies before OFAC can reach a determination. OFAC provides applicants a written response after reaching a determination on each request.

Applicants are encouraged to file specific license applications and requests for interpretive guidance electronically, using [OFAC's License Application portal](#).

Consequences of Noncompliance

Failing to adhere to OFAC sanctions requirements can cause considerable harm to the integrity and effectiveness of U.S. sanctions programs and their related policy objectives. Consequently, civil and criminal penalties for violations can be substantial. OFAC has authority to impose civil penalties for violations, which may vary by sanctions program.

Enforcement Procedures

 **Enforcement Guidelines** OFAC's sanctions enforcement process is governed by the procedures described in OFAC's Economic Sanctions Enforcement Guidelines (the "[Enforcement Guidelines](#)"). (See 31 C.F.R. Part 501, App. A. for the guidelines and current penalty amounts.) OFAC encourages the virtual currency industry to review the Enforcement Guidelines for more information on OFAC's approach to sanctions enforcement.

 **Enforcement Actions** OFAC may take a variety of actions in response to apparent violations. These can include requesting additional information from involved parties; issuing either a "No Action" letter, "Cautionary" letter, "Finding of Violation," or a civil monetary penalty to resolve apparent violations; entering into a settlement with involved parties; or referring the matter to other government agencies, if appropriate, for a criminal investigation. To see a complete list of OFAC's public enforcement actions, please visit our [civil penalties and enforcement information webpage](#).

 **Voluntary Self-Disclosure** For those who believe they may have violated OFAC-administered regulations, OFAC encourages disclosing the apparent violation to OFAC voluntarily. Voluntary self-disclosure to OFAC may be considered a mitigating factor by OFAC in enforcement actions and, pursuant to the Enforcement Guidelines, may result in a 50 percent reduction in the base amount of any proposed civil penalty. Voluntary self-disclosures can be submitted electronically to OFACDisclosures@treasury.gov. Unless the disclosure is an initial disclosure that will be supplemented with additional information, a voluntary self-disclosure submission should contain sufficient detail to afford OFAC a complete understanding of the circumstances surrounding an apparent violation. OFAC's [Office of Compliance and Enforcement \(OCE\) Data Delivery Standards Guidance: Preferred Practices for Productions to OFAC](#) details OFAC's preferred technical standards for formatting electronic document productions for submission. (See [FAQ 13](#))

Sanctions Compliance Best Practices for the Virtual Currency Industry

As a general matter, U.S. persons, including members of the virtual currency industry, are responsible for ensuring they do not engage in unauthorized transactions or dealings with sanctioned persons or jurisdictions.

OFAC strongly encourages a 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 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.

OFAC's [A Framework for OFAC Compliance Commitments](#) provides further detail on the five essential components of a sanctions compliance program:

The Framework also includes an appendix that highlights several of the most common root causes of sanctions violations that OFAC has identified.

All companies in the virtual currency industry, including technology companies, exchangers, administrators, miners, and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers, are encouraged to develop, implement, and routinely update, a tailored, risk-based sanctions compliance program. Such compliance programs generally should include sanctions list and geographic screening and other appropriate measures as determined by the company's unique risk profile.





Management Commitment

Senior management's commitment to a company's sanctions compliance program is one of the most important factors in determining the program's success. Support from senior management is critical to ensure sanctions compliance efforts receive adequate resources and are fully integrated into the company's daily operations. The appropriate tone from the top also helps legitimize the program, empower the company's sanctions compliance personnel, and foster a culture of compliance throughout the company.

The importance of management's commitment to a company's risk-based sanctions compliance program is the same in the virtual currency industry as it is in any other. In many cases, OFAC has observed that members of the virtual currency industry implement OFAC sanctions policies and procedures months, or even years, after commencing operations. Delaying development and implementation of a sanctions compliance program can expose virtual currency companies to a wide variety of potential sanctions risks. It is never too soon to evaluate potential sanctions risks; this includes virtual currency companies that are in the beta testing stage of their operations. Such companies should consider sanctions compliance during the testing and review process so that sanctions compliance can be accounted for as technologies are being developed and prior to launching a new product.

Senior management of companies in the virtual currency industry may consider taking the following steps to demonstrate their support for sanctions compliance:

-  Review and endorse sanctions compliance policies and procedures
-  Ensure adequate resources — including human capital, expertise, information technology, and other resources — support the compliance function
-  Delegate sufficient autonomy and authority to the compliance unit
-  Appoint a dedicated sanctions compliance officer with the requisite technical expertise



Risk Assessment

Sanctions risks are vulnerabilities that, if ignored or mishandled, can lead to violations of OFAC's regulations and subsequent enforcement actions, harm to U.S. foreign policy and national security interests, and negative impacts on a company's reputation and business. OFAC recommends that companies in the virtual currency industry developing a sanctions compliance program conduct a routine and, if appropriate, ongoing risk assessment to identify potential sanctions issues the company is likely to encounter.

While there is no "one-size-fits-all" risk assessment, the exercise should generally include a complete review of the company to assess its touchpoints to foreign jurisdictions or persons. This process allows the company to identify potential areas in which it may, directly or indirectly, engage with OFAC-sanctioned persons, countries, or regions. The results of a risk assessment are integral to developing effective sanctions compliance policies, procedures, internal controls, and training in order to mitigate exposure to sanctions risks.

OFAC encourages members of the virtual currency industry to evaluate their exposure to OFAC sanctions and take steps to minimize their risks — including through development of an appropriate sanctions compliance program — prior to providing services or products to customers. A virtual currency company's risk assessment process should be tailored to the types of products and services offered and the locations in which such products and services are offered. Appropriately customized risk assessments should reflect a company's customer or client base, products, services, supply chain, counterparties, transactions, and geographic locations, and may also include evaluating whether counterparties and partners have adequate compliance procedures.



CASE STUDY:

Diagnosing Risky Relationships

In 2021, OFAC entered into a [settlement agreement](#) with a U.S. virtual currency payment service provider for processing virtual currency transactions between the company's customers and persons located in sanctioned jurisdictions. While the company's sanctions compliance controls included screening its direct customers — merchants in the United States and elsewhere — for a potential nexus to sanctions, the company failed to screen available information about the individuals who used its payment processing platform to buy products from those merchants. Specifically, prior to effecting transactions, the company received information about some of the buyers, such as names, addresses, telephone numbers, email addresses, and, at times, Internet Protocol (IP) addresses. *A comprehensive risk assessment that includes understanding who is accessing a company's platform or services may help members of the virtual currency industry identify the appropriate screening standards to set for each of its products and services.*



Internal Controls

An effective sanctions compliance program will include policies and procedures designed to address the risks identified in a company's risk assessment. These may include controls to identify, interdict, escalate, report (as appropriate), and maintain records for transactions or activities prohibited by OFAC-administered sanctions. An effective sanctions compliance program will enable a company to conduct sufficient due diligence on customers, business partners, and transactions and identify “red flags.” Red flags are indications that illicit activity or compliance breakdowns may be occurring that prompt a company to investigate and take appropriate action. Policies and procedures should be enforced, and weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated to prevent activity that might violate sanctions.

In the virtual currency industry, the internal controls a company implements will depend on, among other things, the products and services the company offers, where the company operates, the locations of its users, and what sanctions-specific risks the company identifies during its risk assessment process. Internal controls often involve the use of industry-specific tools, such as screening, investigation, and transaction monitoring. While OFAC does not require the virtual currency industry to use any particular in-house or third-party software, these can be helpful tools for an effective sanctions compliance program.



CASE STUDY:

Double-Duty Data

One sanctions risk that members of the virtual currency industry face is from users located in sanctioned jurisdictions who try to access virtual currency products and services. Depending on the circumstances, this may result in a sanctions violation. In 2020, a U.S. company that offers digital asset custody, trading, and financing services internationally entered into a [settlement agreement](#) with OFAC for processing virtual currency transactions on behalf of individuals who appeared to be located in sanctioned jurisdictions. Although the company tracked its users' IP addresses when users logged in for security purposes, the company did not use the IP address information it collected to screen for and prevent potential sanctions violations. As a result, the company failed to prevent use of its non-custodial secure digital wallet management service by individuals with IP addresses located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria—all sanctioned jurisdictions at the time. *Implementing internal controls to screen available data and block activity involving certain IP addresses can prevent sanctions violations.*

OFAC recommends the following best practices for virtual currency companies to strengthen internal controls as part of an effective sanctions compliance program:

 **Geolocation Tools** Incorporate geolocation tools and IP address blocking controls. Virtual currency companies with strong sanctions compliance programs should be able to use geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for activity that is prohibited by OFAC's regulations, and not authorized or exempt. Without these internal controls, virtual currency companies may fail to prevent persons who are located in comprehensively sanctioned jurisdictions from accessing their platforms or services to engage in prohibited activity. Analytic tools can identify IP misattribution, for example, by screening IP addresses against known virtual private network (VPN) IP addresses and identifying improbable logins (such as the same user logging in with an IP address in the United States, and then shortly after with an IP address in Japan).

Additionally, virtual currency companies often obtain other information that can alert the company that a particular transaction involves a person located in a sanctioned jurisdiction. This data may come from address information provided by a customer or counterparty, information contained in email addresses, or invoice and other transactional information, among other sources. A company should consider incorporating the review of such information into its sanctions compliance program, even if it was obtained for a different reason — such as for business or security purposes — to ensure the company is utilizing all available information for sanctions compliance purposes.

OFAC has taken enforcement actions against companies in the virtual currency industry that have engaged in prohibited activity because they failed to prevent users in sanctioned jurisdictions from accessing and using their platforms. This was due, in part, to a failure to use the geolocation information in their possession. ([See OFAC's Civil Penalties and Enforcement Information](#) webpage for enforcement actions against virtual currency companies in [2020](#) and [2021](#))

 **Know Your Customer (KYC) Procedures** Obtain information about customers during onboarding and throughout the lifecycle of the customer relationship and use such information to conduct due diligence sufficient to mitigate potential sanctions-related risk. This information can be utilized in the sanctions screening process to prevent violations. For example, information gathering may include the following elements at onboarding, during periodic reviews, and when processing customer transactions:

 **Individuals:** legal name, date of birth, physical and email address, nationality, IP addresses associated with transactions and logins, bank information, and government identification and residency documents

 **Entities:** entity name (including trade and legal name), line of business, ownership information, physical and email address, location information, IP addresses associated with transactions and logins, information about where the entity does business, bank information, and any relevant government documents

Higher-risk customers may warrant additional due diligence. This could include, for example, examining customer transaction history for connections to sanctioned jurisdictions or transactions with virtual currency addresses that have been linked to sanctioned actors. Additionally, information collected in adherence with existing anti-money laundering (AML) obligations, as applicable, may also be helpful in assessing and mitigating sanctions risks. (See FinCEN's [Advisory on Illicit Activity Involving Convertible Virtual Currency](#) for more information regarding applicable AML obligations.)

 **Transaction Monitoring and Investigation** Transaction monitoring and investigation software can be used to identify transactions involving virtual currency addresses or other identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities listed on the SDN List or other sanctions lists, or located in sanctioned jurisdictions. This internal control helps equip virtual currency companies with the ability to prevent transfers to addresses associated with sanctioned persons and avoid violations of U.S. sanctions. Those in the virtual currency industry may also employ transaction monitoring and investigation tools to continually review historical information for such addresses or other identifying information to better understand their exposure to sanctions risks and identify sanctions compliance program deficiencies.

In 2018, OFAC began including certain known virtual currency addresses as identifying information for persons listed on the SDN List. These virtual currency addresses can be searched using the "ID #" field in [OFAC's Sanctions List Search](#) tool. (See FAQs [562](#), [563](#), and [594](#).) As a best practice for risk-based compliance, companies operating in the virtual currency industry should employ tools sufficient to identify and block transactions associated with blocked persons, including transactions associated with those virtual currency addresses included on the SDN List.

Moreover, OFAC's inclusion of virtual currency addresses on the SDN List may assist the industry in identifying other virtual currency addresses that may be associated with blocked persons or otherwise pose sanctions risk, even if those other addresses are not explicitly listed on the SDN List. For example, unlisted virtual currency addresses that share a wallet with a listed virtual currency address may pose sanctions risk because the sharing of a wallet may indicate an association with a blocked person. Similarly, virtual currency companies may consider conducting a historic lookback of transactional activity after OFAC lists a virtual currency address on the SDN List to identify connections to the listed address.

A lookback could also identify connections to unlisted addresses that have previously transacted with the listed address, as such unlisted addresses could also pose sanctions risk depending on the nature of those transactions. Companies in the virtual currency industry may consider deploying blockchain analytics tools that help identify and mitigate these sanctions risks.

✍ Implementing Remedial Measures Upon learning of a weakness in a company's sanctions compliance internal controls (including the discovery of an apparent sanctions violation), virtual currency companies are encouraged to take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated. Consistent with its Enforcement Guidelines, OFAC may consider as a mitigating factor in a potential enforcement action a virtual currency company's implementation of remedial measures taken in response to an apparent violation.

Sanctions Screening: Screening can be an essential part of a virtual currency company's internal controls, and may include geolocation, customer identification, transaction screening, and more. Virtual currency companies should consider implementing the following screening-related best practices into their sanctions compliance programs:

- ✓ Screening customer information against OFAC-administered sanctions lists, including the SDN List, at the time of onboarding
- ✓ Screening transactions to identify addresses, including physical, digital wallet, and IP addresses, and other relevant information with potential links to sanctioned persons or jurisdictions
- ✓ Utilizing screening tools' fuzzy logic capabilities to account for common name variations and misspellings, for example:
 - ✓ Misspellings or alternative spellings related to sanctioned jurisdictions (e.g., "Yalta, Krimea")
 - ✓ Variations on capitalization, spacing, or punctuation for names of persons listed on OFAC sanctions lists (e.g., "Krayinvestbank" may appear on the SDN List, but "Krajinvestbank" or "Kray Invest Bank" may appear in the transaction information provided to a virtual currency company)
- ✓ Ongoing sanctions screening and risk-based re-screening (for example, related to a historical lookback) to account for updated customer information, updates to OFAC sanctions lists, or changes in regulatory requirements

Remediating the Root Causes of Violations In response to OFAC enforcement actions, virtual currency companies have taken action to remediate the root causes of their apparent violations, to identify weaknesses in their internal controls, and to implement new controls to prevent future violations. Some of these remedial measures have included:

- ★ Implementing IP address blocking and email-related restrictions for sanctioned jurisdictions
- ★ Creating a keywords list of a sanctioned jurisdiction's cities and regions to be used when screening KYC information
- ★ Reviewing and updating end-user agreements to include information about U.S. sanctions requirements
- ★ Conducting retroactive batch screening of all users
- ★ Implementing an OFAC-related training program for employees
- ★ Conducting additional sanctions compliance training for all relevant personnel
- ★ Hiring additional compliance staff and a dedicated chief or sanctions compliance officer



Risk Indicators or Red Flags: In addition to screening transaction and other KYC identifying information, virtual currency companies should also consider monitoring transactions and users for risk indicators or “red flags” that may indicate a sanctions nexus. Examples of risk indicators may be individuals or entities who:

- Provide inaccurate or incomplete customer identification or KYC information when attempting to open an account
- Attempt to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction
- Are non-responsive or refuse to provide updated customer identification or KYC information
- Are non-responsive or refuse to provide additional transaction information in response to a virtual currency company's request
- Attempt to transact with a virtual currency address associated with a blocked person or sanctioned jurisdiction

Additionally, as appropriate, “red flags” indicative of money laundering or other illicit financial activity may also be indicative of potential sanctions evasion.



Testing and Auditing

The best way to ensure a sanctions compliance program is working as well as intended is to test the effectiveness of the program. Companies that incorporate a comprehensive, independent, and objective testing or audit function within their sanctions compliance program are equipped to ensure that they are aware of how their programs are performing and what aspects need to be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment.

The size and sophistication of a company may determine whether it conducts internal and external audits of its sanctions compliance program. Some best practices for testing and audit procedures in sanctions compliance programs for the virtual currency industry include:

-  **Sanctions List Screening** Ensure screening of the SDN List and other sanctions lists is functioning effectively and is appropriately flagging transactions for further review
-  **Keyword Screening** Ensure that screening tools are appropriately flagging geographic keywords in connection with KYC-related screening or other transaction screening
-  **IP Blocking** Ensure IP address software is properly preventing users from sanctioned jurisdictions from accessing its products and services
-  **Investigation and Reporting** Review procedures for investigating transactions identified through the screening process as having a potential sanctions nexus (e.g., transactions involving a blocked person or a keyword related to a sanctioned jurisdiction) and procedures for blocked property or rejected transaction reporting to OFAC



Training

Finally, sanctions-specific training is critical to the success of any company's sanctions compliance program. The scope of a company's training will be informed by the size, sophistication, and risk profile of the company. OFAC training should be provided to all appropriate employees, including compliance, management, and customer service personnel, and should be conducted on a periodic basis, and, at a minimum, annually. A well-developed OFAC training program will provide job-specific knowledge based on need, communicate the sanctions compliance responsibilities for each employee, and hold employees accountable for meeting training requirements through the use of assessments.

Effective OFAC training for the virtual currency industry should account for frequent changes and updates to sanctions programs, as well as new and emerging technologies in the virtual currency space.



OFAC Resources

For more information about OFAC sanctions, please visit OFAC’s website where you can find answers to frequently asked questions, including several specific to the virtual currency industry; information about recent designation actions and sanctions list updates; and publications of general licenses, advisories, or other guidance. OFAC issues frequent updates, so we encourage virtual currency companies to sign up for [OFAC’s Recent Actions](#) notifications to receive updates to existing guidance.

Frequently Asked Questions on Virtual Currency Topics

Virtual Currency FAQs	Link
The new FAQ is titled For purposes of OFAC sanctions programs, what do the terms “digital currency,” “digital currency wallet,” “digital currency address,” and “virtual currency” mean?	FAQ 559
Are my OFAC compliance obligations the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency?	FAQ 560
How will OFAC use its existing authorities to sanction those who use digital currencies for illicit purposes?	FAQ 561
How will OFAC identify digital currency-related information on the SDN List?	FAQ 562
What is the structure of a digital currency address on OFAC’s SDN List?	FAQ 563
Is it possible to query a digital currency address using OFAC’s Sanctions List Search tool?	FAQ 594
How do I block virtual currency?	FAQ 646
Should an institution tell its customer that it blocked access to their digital currency and, if so, how does the institution explain it to the customer?	FAQ 647

Venezuela Virtual Currency FAQs	Link
For purposes of Executive Order (E.O.) 13827, “Taking Additional Steps to Deal with the Situation in Venezuela,” of March 19, 2018, are the “petro” and “petro-gold” considered a “digital currency, digital coin, or digital token” that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018?	FAQ 564
For purposes of E.O. 13827, “Taking Additional Steps to Deal with the Situation in Venezuela,” of March 19, 2018, is Venezuela’s traditional fiat currency, bolivar fuerte, considered a “digital currency, digital coin, or digital token” that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018?	FAQ 565
I participated in the pre-sale for a Government of Venezuela-issued “digital currency, digital coin, or digital token” before E.O. 13827, “Taking Additional Steps to Deal with the Situation in Venezuela,” of March 19, 2018, became effective. Am I allowed to sell, trade, use, or otherwise deal in such “digital currency, digital coin, or digital token” on or after the sanctions effective date?	FAQ 566

Contact Information

OFAC’s Compliance Hotline is a resource for the public to contact OFAC for guidance, including general information about OFAC, assistance using OFAC’s Sanctions List Search tool, specific guidance about how to comply with OFAC-administered sanctions programs, and tips for navigating OFAC’s website to find helpful guidance and other information published by OFAC, such as answers to frequently asked questions. We encourage the virtual currency industry to contact OFAC with any questions about this guidance or about complying with sanctions requirements.

By telephone

Toll Free OFAC Compliance Hotline

1-800-540-6322

Electronically

E-mail Hotline

OFAC_Feedback@Treasury.gov

Local OFAC Compliance Hotline

1-202-622-2490

Voluntary Self-Disclosure Submission

OFACDisclosures@Treasury.gov

OFAC’s License Application Status Hotline

1-202-622-2480

Report Submission (if ORS is inaccessible)

OFACReport@treasury.gov

OFAC is committed to engaging with the virtual currency industry to promote understanding of, and compliance with, sanctions requirements.

Resource Sites

OFAC Homepage: www.treasury.gov/ofac

OFAC Contacts Webpage: <https://home.treasury.gov/policy-issues/financial-sanctions/contact-ofac>

OFAC Reporting System: <https://home.treasury.gov/policy-issues/financial-sanctions/ofac-reporting-system>

OFAC Licensing Portal: <https://home.treasury.gov/policy-issues/financial-sanctions/ofac-license-application-page>

Sanctions List Search Tool: <https://sanctionssearch.ofac.treas.gov/>

SDN List: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas>

Consolidated Sanctions List (Non-SDN Lists):

<https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists>

Other OFAC Sanctions Lists: <https://home.treasury.gov/policy-issues/financial-sanctions/other-ofac-sanctions-lists>

OFAC-Administered Sanctions Programs and Country Information:

<https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information>

OFAC FAQs: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs>

OFAC Recent Actions: <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions>

Economic Sanctions Enforcement Guidelines – Appendix A to Part 501: https://home.treasury.gov/system/files/126/fr74_57593.pdf

A Framework for OFAC Compliance Commitments: https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

Office of Compliance and Enforcement (“OCE”) Data Delivery Standards Guidance: Preferred Practices for Productions to OFAC:

<https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information/ofac-office-of-compliance-and-enforcement-data-delivery-standards-guidance-preferred-practices-for-productions-to-ofac>

Civil Penalties and Enforcement Information:

<https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>

Guidance on the North Korean Cyber Threat: https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf



OFAC

Office of Foreign Assets Control

This document is explanatory only and does not have the force of law. The guidance contained herein may be subject to frequent change and does not supplement or modify the statutes, regulations, executive orders, or other authorities that govern sanctions administered by OFAC. See Title 31, Chapter V of the Code of Federal Regulations and <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information> for legally binding provisions governing OFAC-administered sanctions.

