Seasif
Holding

OFAC Manual Policy

Seasif Holding LTD

April 2026

A Framework for OFAC Compliance Commitments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities in accordance with national security and foreign policy goals and objectives.

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP). While each risk-based SCP will vary depending on a variety of factors—including the company's size and sophistication, products and services, customers and counterparties, and geographic locations—each program 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.

If after conducting an investigation and determining that a civil monetary penalty ("CMP") is the appropriate administrative action in response to an apparent violation, the Office of Compliance and Enforcement (OCE) will determine which of the following or other elements should be incorporated into the subject person's SCP as part of any accompanying settlement agreement, as appropriate. As in all enforcement cases, OFAC will evaluate a subject person's SCP in a manner consistent with the Economic Sanctions Enforcement Guidelines (the "Guidelines").

When applying the Guidelines to a given factual situation, OFAC will consider favorably subject persons that had effective SCPs at the time of an apparent violation. For example, under General Factor E (compliance program), OFAC may consider the existence, nature, and adequacy of an SCP, and when appropriate, may mitigate a CMP on that basis. Subject persons that have implemented effective SCPs that are predicated on the five essential components of compliance may also benefit from further mitigation of a CMP pursuant to General Factor F (remedial response) when the SCP results in remedial steps being taken.

Finally, OFAC may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed "egregious."

This document is intended to provide organizations with a framework for the five essential components of a risk-based SCP, and contains an appendix outlining several of the root causes that have led to apparent violations of the sanctions programs that OFAC administers. OFAC recommends all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and enhance their respective SCPs, when and as appropriate.

MANAGEMENT COMMITMENT

Senior Management's commitment to, and support of, an organization's risk-based SCP is one of the most important factors in determining its success. This support is essential in ensuring the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

General Aspects of an SCP: Senior Management Commitment

Senior management commitment to supporting an organization's SCP is a critical factor in determining the success of the SCP. Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel's authority within an organization. The term "senior management" may differ among various organizations, but typically the term should include senior leadership, executives, and/or the board of directors.

I. Senior management has reviewed and approved the organization's SCP.

II. Senior management ensures that its compliance unit(s) is/are delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the organization's OFAC risk. As part of this effort, senior management ensures the existence of direct reporting lines between the SCP function and senior management, including routine and periodic meetings between these two elements of the organization.

III. Senior management has taken, and will continue to take, steps to ensure that the organization's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

These efforts could generally be measured by the following criteria:

A. The organization has appointed a dedicated OFAC sanctions compliance officer[1];
B. The quality and experience of the personnel dedicated to the SCP, including: (i) the technical knowledge and expertise of these personnel with respect to OFAC's regulations, processes, and actions; (ii) the ability of these personnel to understand complex financial and commercial activities, apply their knowledge of OFAC to these items, and identify OFAC-related issues, risks, and prohibited activities; and (iii) the efforts to ensure that personnel dedicated to the SCP have sufficient experience and an appropriate position within the organization, and are an integral component to the organization's success; and

[1] This may be the same person serving in other senior compliance positions, e.g., the Bank Secrecy Act Officer or an Export Control Officer, as many institutions, depending on size and complexity, designate a single person to oversee all areas of financial crimes or export control compliance.

C. Sufficient control functions exist that support the organization's SCP—including but not limited to information technology software and systems—that adequately address the organization's OFAC-risk assessment and levels.

IV. Senior management promotes a "culture of compliance" throughout the organization.

These efforts could generally be measured by the following criteria:

A. The ability of personnel to report sanctions related misconduct by the organization or its personnel to senior management without fear of reprisal.
B. Senior management messages and takes actions that discourage misconduct and prohibited activities, and highlight the potential repercussions of non-compliance with OFAC sanctions; and
C. The ability of the SCP to have oversight over the actions of the entire organization, including but not limited to senior management, for the purposes of compliance with OFAC sanctions.

V. Senior management demonstrates recognition of the seriousness of apparent violations of the laws and regulations administered by OFAC, or malfunctions, deficiencies, or failures by the organization and its personnel to comply with the SCP's policies and procedures, and implements necessary measures to reduce the occurrence of apparent violations in the future. Such measures should address the root causes of past apparent violations and represent systemic solutions whenever possible.

RISK ASSESSMENT

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of OFAC's regulations and negatively affect an organization's reputation and business. OFAC recommends that organizations take a risk-based approach when designing or updating an SCP. One of the central tenets of this approach is for organizations to conduct a routine, and if appropriate, ongoing "risk assessment" for the purposes of identifying potential OFAC issues they are likely to encounter. As described in detail below, the results of a risk assessment are integral in informing the SCP's policies, procedures, internal controls, and training in order to mitigate such risks.

While there is no "one-size-fits all" risk assessment, the exercise should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world. This process allows the organization to identify potential areas in which it may, directly or indirectly, engage with OFAC-prohibited persons, parties, countries, or regions. For example, an organization's SCP may conduct an assessment of the following: (i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties. Risk assessments and sanctions-related due diligence is also important

during mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations.

General Aspects of an SCP: Conducting a Sanctions Risk Assessment

A fundamental element of a sound SCP is the assessment of specific clients, products, services, and geographic locations in order to determine potential OFAC sanctions risk. The purpose of a risk assessment is to identify inherent risks in order to inform risk-based decisions and controls. The Annex to Appendix A to 31 C.F.R. Part 501, OFAC's Economic Sanctions Enforcement Guidelines, provides an OFAC Risk Matrix that may be used by financial institutions or other entities to evaluate their compliance programs:

I. The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. Such risks could be posed by its clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization. As appropriate, the risk assessment will be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.

A. In assessing its OFAC risk, organizations should leverage existing information to inform the process. In turn, the risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction. This may include:

1. On-boarding: The organization develops a sanctions risk rating for customers, customer groups, or account relationships, as appropriate, by leveraging information provided by the customer (for example, through a Know Your Customer or Customer Due Diligence process) and independent research conducted by the organization at the initiation of the customer relationship. This information will guide the timing and scope of future due diligence efforts. Important elements to consider in determining the sanctions risk rating can be found in OFAC's risk matrices.
2. Mergers and Acquisitions (M&A): As noted above, proper risk assessments should include and encompass a variety of factors and data points for each organization. One of the multitude of areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are mergers and acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is completed, the

organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.

II. The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.

INTERNAL CONTROLS

An effective SCP should include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessments. Policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis.

Given the dynamic nature of U.S. economic and trade sanctions, a successful and effective SCP should be capable of adjusting rapidly to changes published by OFAC. These include the following: (i) updates to OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"), the Sectoral Sanctions Identification List ("SSI List"), and other sanctions-related lists; (ii) new, amended, or updated sanctions programs or prohibitions imposed on targeted foreign countries, governments, regions, or persons, through the enactment of new legislation, the issuance of new Executive orders, regulations, or published OFAC guidance or other OFAC actions; and (iii) the issuance of general licenses.

General Aspects of an SCP: Internal Controls

Effective OFAC compliance programs generally include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance, and minimize the risks identified by an entity's OFAC risk assessments. Policies and procedures should be enforced, and weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated in order to prevent activity that might violate the sanctions programs administered by OFAC.

I. The organization has designed and implemented written policies and procedures outlining the SCP. These policies and procedures are relevant to the organization, capture the organization's day-to-day operations and procedures, are easy to follow, and designed to prevent employees from engaging in misconduct.

II. **The organization has implemented internal controls that adequately address the results of its OFAC risk assessment and profile. These internal controls should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC. To the extent information technology solutions factor into the organization's internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization's risk profile and compliance needs, and the organization routinely tests the solutions to ensure effectiveness.**

III. **The organization enforces the policies and procedures it implements as part of its OFAC compliance internal controls through internal and/or external audits.**

IV. **The organization ensures that its OFAC-related recordkeeping policies and procedures adequately account for its requirements pursuant to the sanctions programs administered by OFAC.**

V. **The organization ensures that, upon learning of a weakness in its internal controls pertaining to OFAC compliance, it will 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.**

VI. **The organization has clearly communicated the SCP's policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the organization.**

VII. **The organization has appointed personnel for integrating the SCP's policies and procedures into the daily operations of the company or corporation. This process includes consultations with relevant business units, and confirms the organization's employees understand the policies and procedures.**

TESTING AND AUDITING

Audits assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. A comprehensive and objective testing or audit function within an SCP ensures that an organization identifies program weaknesses and deficiencies, and it is the organization's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level.

General Aspects of an SCP: Testing and Auditing

A comprehensive, independent, and objective testing or audit function within an SCP ensures that entities are aware of where and how their programs are performing and should be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment, as appropriate. Testing or audit, whether conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and identify weaknesses and deficiencies within a compliance program.

I. **The organization commits to ensuring that the testing or audit function is accountable to senior management, is independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.**

II. **The organization commits to ensuring that it employs testing or audit procedures appropriate to the level and sophistication of its SCP and that this function, whether deployed internally or by an external party, reflects a comprehensive and objective assessment of the organization's OFAC-related risk assessment and internal controls.**

III. **The organization ensures that, upon learning of a confirmed negative testing result or audit finding pertaining to its SCP, it will 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.**

TRAINING

An effective training program is an integral component of a successful SCP. The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments.

General Aspects of an SCP: Training

An adequate training program, tailored to an entity's risk profile and all appropriate employees and stakeholders, is critical to the success of an SCP.

I. **The organization commits to ensuring that its OFAC-related training program provides adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, suppliers, business partners, and counterparties) in order to support the organization's OFAC compliance efforts. Such training should be further tailored to high-risk employees within the organization.**

II. **The organization commits to provide OFAC-related training with a scope that is appropriate for the products and services it offers; the customers, clients, and partner relationships it maintains; and the geographic regions in which it operates.**

III. **The organization commits to providing OFAC-related training with a frequency that is appropriate based on its OFAC risk assessment and risk profile.**

IV. **The organization commits to ensuring that, upon learning of a confirmed negative testing result or audit finding, or other deficiency pertaining to its SCP, it will take immediate and effective action to provide training to or other corrective action with respect to relevant personnel.**

V. **The organization's training program includes easily accessible resources and materials that are available to all applicable personnel.**

Root Causes of OFAC Sanctions Compliance Program Breakdowns or Deficiencies Based on Assessment of Prior OFAC Administrative Actions

Since its publication of the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, App. A (the "Guidelines"), OFAC has finalized numerous public enforcement actions in which it identified deficiencies or weaknesses within the subject person's SCP. These items, which are provided in a non-exhaustive list below, are provided to alert persons subject to U.S. jurisdiction, including entities that conduct business in or with the United States, U.S. persons, or U.S.-origin goods or services, about several specific root causes associated with apparent violations of the regulations it administers in order to assist them in designing, updating, and amending their respective SCP.

I. Lack of a Formal OFAC SCP

OFAC regulations do not require a formal SCP; however, OFAC encourages organizations subject to U.S. jurisdiction (including but not limited to those entities that conduct business in, with, or through the United States or involving U.S.-origin goods, services, or technology), and particularly those that engage in international trade or transactions or possess any clients or counter-parties located outside of the United States, to adopt a formal SCP. OFAC has finalized numerous civil monetary penalties since publicizing the Guidelines in which the subject person's lack of an SCP was one of the root causes of the sanctions violations identified during the course of the investigation. In addition, OFAC frequently identified this element as an aggravating factor in its analysis of the General Factors associated with such administrative actions.

II. Misinterpreting, or Failing to Understand the Applicability of, OFAC's Regulations

Numerous organizations have committed sanctions violations by misinterpreting OFAC's regulations, particularly in instances in which the subject person determined the transaction, dealing, or activity at issue was either not prohibited or did not apply to their organization or operations. For example, several organizations have failed to appreciate or consider (or, in some instances, actively disregarded) the fact that OFAC sanctions applied to their organization based on their status as a U.S. person, a U.S.-owned or controlled subsidiary (in the Cuba and Iran programs), or dealings in or with U.S. persons, the U.S. financial system, or U.S.-origin goods and technology.

With respect to this specific root cause, OFAC's administrative actions have typically identified additional aggravating factors, such as reckless conduct, the presence of numerous warning signs that the activity at issue was likely prohibited, awareness by the organization's management of the conduct at issue, and the size and sophistication of the subject person.

III. Facilitating Transactions by Non-U.S. Persons (Including Through or By Overseas Subsidiaries or Affiliates)

Multiple organizations subject to U.S. jurisdiction—specifically those with foreign-based operations and subsidiaries located outside of the United States—have engaged in transactions or activity that violated OFAC's regulations by referring business opportunities to, approving or signing off on transactions conducted by, or otherwise facilitating dealings

between their organization's non-U.S. locations and OFAC-sanctioned countries, regions, or persons. In many instances, the root cause of these violations stems from a misinterpretation or misunderstanding of OFAC's regulations. Companies and corporations with integrated operations, particularly those involving or requiring participation by their U.S.-based headquarters, locations, or personnel, should ensure any activities they engage in (i.e., approvals, contracts, procurement, etc.) are compliant with OFAC's regulations.

IV. Exporting or Re-exporting U.S.-origin Goods, Technology, or Services to OFAC-Sanctioned Persons or Countries

Non-U.S. persons have repeatedly purchased U.S.-origin goods with the specific intent of re-exporting, transferring, or selling the items to a person, country, or region subject to OFAC sanctions. In several instances, this activity occurred despite warning signs that U.S. economic sanctions laws prohibited the activity, including contractual language expressly prohibiting any such dealings. OFAC's public enforcement actions in this area have generally been focused on companies or corporations that are large or sophisticated, engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, utilized non-routine business practices, and—in several instances—concealed their activity in a willful or reckless manner.

V. Utilizing the U.S. Financial System, or Processing Payments to or through U.S. Financial Institutions, for Commercial Transactions Involving OFAC-Sanctioned Persons or Countries

Many non-U.S. persons have engaged in violations of OFAC's regulations by processing financial transactions (almost all of which have been denominated in U.S. Dollars) to or through
U.S. financial institutions that pertain to commercial activity involving an OFAC-sanctioned country, region, or person. Although no organizations subject to U.S. jurisdiction may be involved in the underlying transaction—such as the shipment of goods from a third-country to an OFAC-sanctioned country—the inclusion of a U.S. financial institution in any payments associated with these transactions often results in a prohibited activity (e.g., the exportation or re-exportation of services from the United States to a comprehensively sanctioned country, or dealing in blocked property in the United States). OFAC has generally focused its enforcement investigations on persons who have engaged in willful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-U.S. or U.S. financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organization's management, caused significant harm to U.S. sanctions program objectives, and were large or sophisticated organizations.

VI. Sanctions Screening Software or Filter Faults

Many organizations conduct screening of their customers, supply chain, intermediaries, counter-parties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the SDN List or SSI List, failed to include pertinent identifiers such as SWIFT Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties—particularly in instances in which the organization is domiciled or conducts business in geographies that frequently utilize such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.),

VII. Improper Due Diligence on Customers/Clients (e.g., Ownership, Business Dealings, etc.)

One of the fundamental components of an effective OFAC risk assessment and SCP is conducting due diligence on an organization's customers, supply chain, intermediaries, and counter-parties. Various administrative actions taken by OFAC involved improper or incomplete due diligence by a company or corporation on its customers, such as their ownership, geographic location(s), counter-parties, and transactions, as well as their knowledge and awareness of OFAC sanctions.

VIII. De-Centralized Compliance Functions and Inconsistent Application of an SCP

While each organization should design, develop, and implement its risk-based SCP based on its own characteristics, several organizations subject to U.S. jurisdiction have committed apparent violations due to a de-centralized SCP, often with personnel and decision-makers scattered in various offices or business units. In particular, violations have resulted from this arrangement due to an improper interpretation and application of OFAC's regulations, the lack of a formal escalation process to review high-risk or potential OFAC customers or transactions, an inefficient or incapable oversight and audit function, or miscommunications regarding the organization's sanctions-related policies and procedures.

IX. Utilizing Non-Standard Payment or Commercial Practices

Organizations subject to U.S. jurisdiction are in the best position to determine whether a particular dealing, transaction, or activity is proposed or processed in a manner that is consistent with industry norms and practices. In many instances, organizations attempting to evade or circumvent OFAC sanctions or conceal their activity will implement non-traditional business methods in order to complete their transactions.

X. Individual Liability

In several instances, individual employees—particularly in supervisory, managerial, or executive-level positions—have played integral roles in causing or facilitating violations of the regulations administered by OFAC. Specifically, OFAC has identified scenarios involving U.S.-owned or controlled entities operating outside of the United States, in which supervisory, managerial or executive employees of the entities conducted or facilitated dealings or transactions with OFAC-sanctioned persons, regions, or countries, notwithstanding the fact that
the U.S. entity had a fulsome sanctions compliance program in place. In some of these cases, the employees of the foreign entities also made efforts to obfuscate and conceal their activities from others within the corporate organization, including compliance personnel, as well as from regulators or law enforcement. In such circumstances, OFAC will consider using its enforcement authorities not only against the violating entities, but against the individuals as well.

Office of Foreign Assets Control — Overview

Objective. *Assess the bank's risk-based Office of Foreign Assets Control (OFAC) compliance program to evaluate whether it is appropriate for the bank's OFAC risk, taking into consideration its products, services, customers, entities, transactions, and geographic locations.*

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime.

OFAC acts under Presidential wartime and national emergency powers, as well as various authorities granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.[148] Many of these sanctions are based on United Nations and other international mandates; therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the national security interests of the United States.

On November 9, 2009, OFAC issued a final rule entitled "Economic Sanctions Enforcement Guidelines" in order to provide guidance to persons subject to its regulations. The document explains the procedures that OFAC follows in determining the appropriate enforcement response to apparent violations of its regulations. Some enforcement responses may result in the issuance of a civil penalty that, depending on the sanctions program affected, may be as much as $250,000 per violation or twice the amount of a transaction, whichever is greater.
The Guidelines outline the various factors that OFAC takes into account when making enforcement determinations, including the adequacy of a compliance program in place within an institution to ensure compliance with OFAC regulations.[149]

All U.S. persons,[150] including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations.[151] The federal banking agencies

---

[148] Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 *et seq.*; Antiterrorism and Effective Death Penalty Act (AEDPA), 8 USC 1189, 18 USC 2339B; United Nations Participation Act (UNPA), 22 USC 287c; Cuban Democracy Act (CDA), 22 USC 6001–10; The Cuban Liberty and Democratic Solidarity Act (Libertad Act), 22 USC 6021–91; The Clean Diamonds Trade Act, Pub. L. No. 108-19; Foreign Narcotics Kingpin Designation Act (Kingpin Act), 21 USC 1901–1908, 8 USC 1182; Burmese Freedom and Democracy Act of 2003, Pub. L. No. 108–61, 117 Stat. 864 (2003); The Foreign Operations, Export Financing and Related Programs Appropriations Act, Sec 570 of Pub.
L. No. 104-208, 110 Stat. 3009-116 (1997); The Iraqi Sanctions Act, Pub. L. No. 101-513, 104 Stat. 2047-55
(1990); The International Security and Development Cooperation Act, 22 USC 2349 aa8–9; The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000).

[149] Refer to 73 *Fed. Reg.* 57593 (November 9, 2009) for additional information (also available on the OFAC Web site).

[150] All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and

evaluate OFAC compliance programs to ensure that all banks subject to their supervision comply with the sanctions.[152] Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries.

OFAC encourages banks to take a risk-based approach to designing and implementing an OFAC compliance program. In general, the regulations that OFAC administers require banks to do the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party to the transaction, it must be blocked. The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account.[153] A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

---

their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

[151] Additional information is provided in *Foreign Assets Control Regulations for the Financial Community*, which is available on the OFAC Web site.

[152] 31 CFR Chapter V.

[153] A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDN), involving an export to a company in Sudan that also is not an SDN. Because the Sudanese Sanctions Regulations would only require blocking transactions with the Government of Sudan or an SDN, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute the exportation of services to Sudan, which is prohibited, the U.S. bank cannot process the transaction and would simply reject the transaction.

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's CIP regulation (31 CFR 1020.220(a)(4)) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to the core overview section, "Customer Identification Program," page 47, for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from the OFAC Web site. Before processing transactions that may be covered under a general license, banks should verify that such transactions meet the relevant criteria of the general license.[154]

Specific licenses are issued on a case-by-case basis.[155] A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions generally limited to a specified time period. To receive a specific license, the person or

[154] License information for a particular sanction program is available on the OFAC Web site or by contacting OFAC's Licensing area at (202) 622-2480.

[155] Applications for a specific license may be submitted either online from the OFAC Web site, or in writing to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms to OFAC's internal licensing policies and U.S. foreign policy objectives, the license generally is issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms and conditions of the license (including the effective dates of the license), and may wish to obtain and retain a copy of the authorizing license for recordkeeping purposes.

OFAC Reporting

Banks must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[156] Once assets or funds are blocked, they should be placed in a separate blocked account. Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence.

Banks must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN and other lists, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on the OFAC Web site.[158]

OFAC Compliance Program

While not required by specific regulation, but as a matter of sound banking practice and in order to mitigate the risk of noncompliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program that is commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank.

OFAC Risk Assessment

A fundamental element of a sound OFAC compliance program is the bank's assessment of its specific product lines, customer base, and nature of transactions and identification of higher-risk areas for potential OFAC sanctions risk. The initial identification of higher-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, banks should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and

[156] The annual report is to be filed on form TD F 90-22.50.

[157] Reporting, procedures, and penalties regulations, 31 CFR Part 501.

[158] This information is available on the OFAC Web site, or by contacting OFAC's hot line at (202) 622-2490 or toll-free at (800) 540-6322.

processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the bank includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, depends on the bank's risk profile and available technology.

Based on the bank's OFAC risk profile for each area and available technology, the bank should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser, or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a bank knows or has reason to know that a transaction party on a check is an OFAC target, the bank's processing of the transaction would expose the bank to liability, especially personally handled transactions in a higher-risk area. For example, if a bank knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a bank should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border ACH transactions.
- Commercial letters of credit and other trade finance products.
- Transactional electronic banking.
- Foreign correspondent bank accounts.
- Payable through accounts.
- Concentration accounts.
- International private banking.
- Overseas branches or subsidiaries.

Appendix M ("Quantity of Risk — OFAC Procedures") provides guidance to examiners on assessing OFAC risks facing a bank. The risk assessment can be used to assist the examiner in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its Web site under "Frequently Asked Questions."[159]

Once the bank has identified its areas with higher OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, banks are encouraged to periodically reassess their OFAC risks.

Internal Controls

An effective OFAC compliance program should include internal controls for identifying suspect accounts and transactions, as well as reporting blocked and rejected transactions to OFAC. Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The bank's policies, procedures, and processes should address how the bank identifies and reviews transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing names provided on the OFAC list with the names in the bank's files or on transactions and for identifying transactions or accounts involving sanctioned countries. The bank's policies, procedures, and processes should also address how the bank determines whether an initial OFAC hit is a valid match or a false hit.[160] A high volume of false hits may indicate a need to review the bank's interdiction program.

The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the bank's interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Banks with lower OFAC risk and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology. In addition, banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible

[159] This guidance is available on the OFAC Web site.

[160] Due diligence steps for determining a valid match are provided in *Using OFAC's Hot line* on the OFAC Web site.

enforcement action. In addition, banks should have policies, procedures, and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk. For example, banks with a lower OFAC risk level may periodically (e.g., weekly, monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and noncustomer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the bank should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of the bank's OFAC compliance program, to be a factor in determining the appropriate enforcement response to an apparent violation of OFAC regulations.[161] The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.

If a bank uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, banks should have a written agreement in place and establish adequate controls and review procedures for such relationships.

Updating OFAC lists. A bank's OFAC compliance program should include policies, procedures, and processes for timely updating of the lists of sanctioned countries and blocked entities, and individuals, and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Iran and Cuba, foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening Automated Clearing House (ACH) transactions. ACH transactions may involve persons or parties subject to the sanctions programs administered by OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216, for additional guidance. OFAC has clarified its interpretation of the application of OFAC's rules for domestic and cross-border ACH transactions and provided more detailed guidance on international ACH transactions.[162]

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to ascertain that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC regulations.

If an ODFI receives domestic ACH transactions that its customer has already batched, the ODFI is not responsible for unbatching those transactions to ensure that no transactions violate OFAC's regulations. If an ODFI unbatches a file originally received

[161] Refer to 74 *Fed. Reg.* 57593 (November 9, 2009), *Economic Sanctions Enforcement Guidelines*. Further information is available on the OFAC Web site.

[162] Refer to Guidance to National Automated Clearing House Association (NACHA) on cross-border ACH transactions.

from the Originator in order to process "on-us" transactions, that ODFI is responsible for the OFAC compliance for the on-us transactions because it is acting as both the ODFI and the RDFI for those transactions. ODFIs acting in this capacity should already know their customers for the purposes of OFAC and other regulatory requirements. For the residual unbatched transactions in the file that are not "on-us," as well as those situations where banks deal with unbatched ACH records for reasons other than to strip out the on-us transactions, banks should determine the level of their OFAC risk and develop appropriate policies, procedures, and processes to address the associated risks. Such policies might involve screening each unbatched ACH record. Similarly, banks that have relationships with third-party service providers should assess those relationships and their related ACH transactions to ascertain the bank's level of OFAC risk and to develop appropriate policies, procedures, and processes to mitigate that risk.

With respect to cross-border screening, similar but somewhat more stringent OFAC obligations hold for International ACH transactions (IAT). In the case of inbound IATs, and regardless of whether the OFAC flag in the IAT is set, an RDFI is responsible for compliance with OFAC sanctions programs. For outbound IATs, however, the ODFI cannot rely on OFAC screening by an RDFI outside of the United States. In these situations, the ODFI must exercise increased diligence to ensure that illegal transactions are not processed.

Due diligence for an inbound or outbound IAT may include screening the parties to a transaction, as well as reviewing the details of the payment field information for an indication of a sanctions violation, investigating the resulting hits, if any, and ultimately blocking or rejecting the transaction, as appropriate. Refer to the expanded overview section, "Automated Clearing House Transactions," page 216, for additional guidance.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[163]

In guidance issued on March 10, 2009, OFAC authorized institutions in the United States when they are acting as an ODFI/Gateway Operator (GO) for inbound IAT debits to reject transactions that appear to involve blockable property or property interests.[164] The guidance further states that to the extent that an ODFI/GO screens inbound IAT debits for possible OFAC violations prior to execution and in the course of such screening discovers a potential OFAC violation, the suspect transaction is to be removed from the batch for further investigation. If the ODFI/GO determines that the transaction does appear to violate OFAC regulations, the ODFI/GO should refuse to process the transfer. The procedure applies to transactions that would normally be blocked as well as to transactions that would normally be rejected for OFAC purposes based on the information in the payment.

Reporting. An OFAC compliance program should also include policies, procedures, and processes for handling validly blocked or rejected items under the various sanctions programs.

---

[163] Refer to the FFIEC *Information Technology Examination Handbook's* Retail Payment Systems booklet.

[164] Refer to the NACHA Web site.

When there is a question about the validity of an interdiction, banks can contact OFAC by phone or e-hot line for guidance. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the management of blocked accounts. Banks are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a bank acquires or merges with another bank, both banks should take into consideration the need to review and maintain such records and information.

Banks no longer need to file SARs based solely on blocked narcotics- or terrorism-related transactions, as long as the bank files the required blocking report with OFAC. However, because blocking reports require only limited information, if the bank is in possession of additional information not included on the OFAC blocking report, a separate SAR should be filed with FinCEN that would include such information. In addition, the bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.[165]

Maintaining license information. OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file. This allows the bank to verify whether a customer is initiating a legal transaction. Banks should also be aware of the expiration date on the OFAC license. If it is unclear whether a particular transaction would be authorized under the terms of the license, the bank should contact OFAC. Maintaining copies of OFAC licenses also is useful when another bank in the payment chain requests verification of a license's validity. Copies of OFAC licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every bank should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. For large banks, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller banks, the audit should be consistent with the bank's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program.

Responsible Individual

It is recommended that every bank designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC compliance program, including changes or updates to the various sanctions programs, and the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

---

[165] Refer to FinCEN Release Number 2004-02, *Unitary Filing of Suspicious Activity and Blocking Reports*, 69 *Fed. Reg.* 76847 (December 23, 2004).

Training

The bank should provide adequate training for all appropriate employees on its OFAC compliance program, procedures and processes. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.

OFAC RISK MATRIX

The following risk matrix is found in the Federal Register at 31 CFR Part 501, and is provided to assist financial institutions in identifying and evaluating their specific OFAC Risk Factors.

Low	Moderate	High
Stable, well-known customer base in a localized environment	Customer base changing due to branching, merger, or acquisition in the domestic market	A large, fluctuating client base in an international environment.
Few high-risk customers; these may include nonresident aliens, foreign customers (including accounts with U.S. powers of attorney), and foreign commercial customers	A moderate number of high-risk customers	A large number of high-risk customers.
No overseas branches and no correspondent accounts with foreign banks	Overseas branches or correspondent accounts with foreign banks	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic services (e.g., e-banking) offered, or products available are purely informational or non-transactional	The institution offers limited electronic (e.g., e-banking) products and services	The institution offers a wide array of electronic (e.g., e-banking) products and services (i.e., account transfers, e-bill payment, or accounts opened via the Internet).

Limited number of funds transfers for customers and non-customers, limited third-party transactions, and no international funds transfers	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts	A high number of customer and non-customer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt	Limited other types of international transactions	A high number of other types of international transactions.
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation	A small number of recent actions (i.e., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the institution addressed the issues and is not at risk of similar violations in the future	Multiple recent actions by OFAC, where the institution has not addressed the issues, thus leading to an increased risk of the institution undertaking similar violations in the future.
Management has fully assessed the institution's level of risk based on its customer base and product lines. This understanding of risk and strong commitment to OFAC compliance is satisfactorily communicated throughout the organization	Management exhibits a reasonable understanding of the key aspects of OFAC compliance and its commitment is generally clear and satisfactorily communicated throughout the organization, but it may lack a program appropriately tailored to risk	Management does not understand, or has chosen to ignore, key aspects of OFAC compliance risk. The importance of compliance is not emphasized or communicated throughout the organization.

The board of directors, or board committee, has approved an OFAC compliance program that includes policies, procedures, controls, and information systems that are adequate, and consistent with the institution's OFAC risk profile	The board has approved an OFAC compliance program that includes most of the appropriate policies, procedures, controls, and information systems necessary to ensure compliance, but some weaknesses are noted	The board has not approved an OFAC compliance program, or policies, procedures, controls, and information systems are significantly deficient.
Staffing levels appear adequate to properly execute the OFAC compliance program	Staffing levels appear generally adequate, but some deficiencies are noted	Management has failed to provide appropriate staffing levels to handle workload.
Authority and accountability for OFAC compliance are clearly defined and enforced, including the designation of a qualified OFAC officer	Authority and accountability are defined, but some refinements are needed. A qualified OFAC officer has been designated	Authority and accountability for compliance have not been clearly established. No OFAC compliance officer, or an unqualified one, has been appointed. The role of the OFAC officer is unclear.
Training is appropriate and effective based on the institution's risk profile, covers applicable personnel, and provides necessary up-to-date information and resources to ensure compliance	Training is conducted and management provides adequate resources given the risk profile of the organization; however, some areas are not covered within the training program	Training is sporadic and does not cover important regulatory and risk areas or is nonexistent.
The institution employs strong quality control methods	The institution employs limited quality control methods	The institution does not employ quality control methods.

Sanctions Compliance Guidance for the Virtual Currency Industry

Contents:

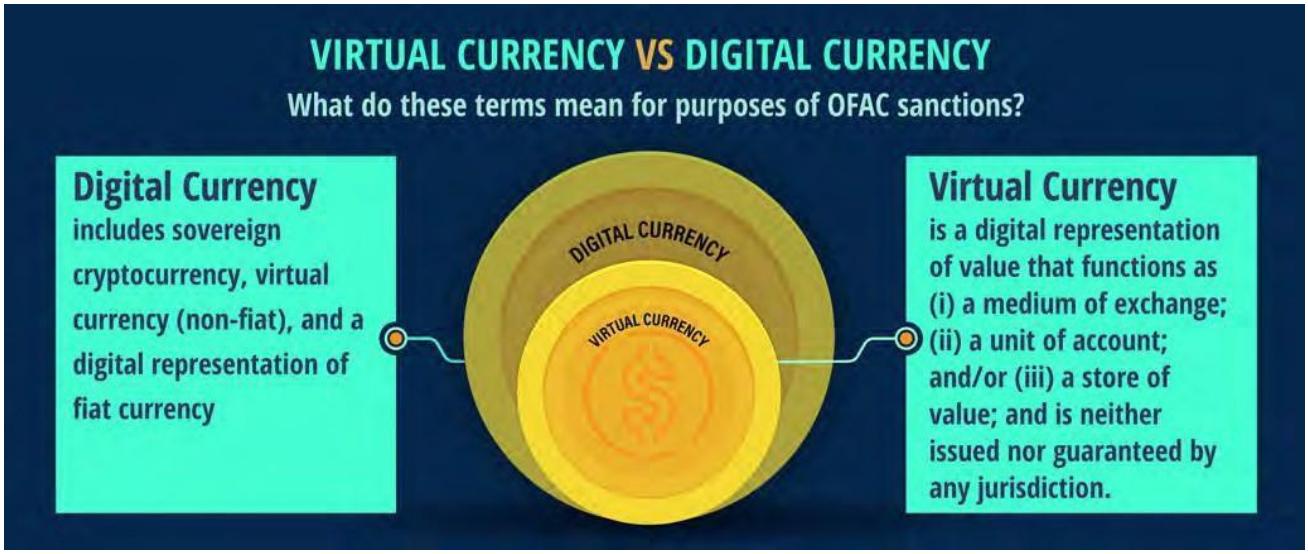
INTRODUCTION

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.



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

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

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	
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**
Local OFAC Compliance Hotline **1-202-622-2490**
OFAC's License Application Status Hotline **1-202-622-2480**

Electronically

E-mail Hotline OFAC_Feedback@Treasury.gov
Voluntary Self-Disclosure Submission OFACDisclosures@Treasury.gov
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

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[3]

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through virtual currency, in exchange for a

[1] This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive, or as imposing requirements under U.S. law, or otherwise addressing any requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

[2] This advisory updates and supersedes OFAC's *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* of October 1, 2020.

[3] This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation (FBI), there was a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020.[4] Ransomware attacks are carried out against private and governmental entities of all sizes and in all sectors, including organizations operating critical infrastructure, such as hospitals. Often attacks also take place against vulnerable entities such as school districts and smaller businesses, in part due to the attacker's assumption that such victims may have fewer resources to invest in cyber protection and will make quick payment to restore services.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.[5] OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.[6]

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two virtual currency addresses used to funnel SamSam ransomware proceeds.[7]

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.[8]

---

[4] *Compare* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf, *with* Federal Bureau of Investigation, Internet Crime Complaint Center, *2020 Internet Crime Report*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[5] Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), available at https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[6] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

[7] Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.

[8] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at https://home.treasury.gov/news/press-releases/sm774.

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.[9]

In September 2021, OFAC designated SUEX OTC, S.R.O. ("SUEX"), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors, involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions showed that over 40% of SUEX's known transaction history was associated with illicit actors.[10]

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.[11]

Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims.
For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks. Moreover, there is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[12] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a

[9] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at https://home.treasury.gov/news/press-releases/sm845.
[10] Press Release, U.S. Dept. of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0364.
[11] Federal charges have also been brought in connection with each of the aforementioned ransomware schemes. *See*, e.g., Press Release, U.S. Dept. of Justice, Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware (Dec. 5, 2019), available at https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens; and Press Release U.S. Dept. of Justice, Three North Korean Military Hackers Indicted in Wide Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (Feb. 17, 2021), available at https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks and#:~:text=A%20federal%20indictment%20unsealed%20today,and%20companies%2C%20to%20create%20.
[12] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

violation under IEEPA, including a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC's Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)[13] provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Enforcement responses range from non-public responses, including issuing a No Action Letter or a Cautionary Letter, to public responses, such as civil monetary penalties.

Sanctions Compliance Program and Defensive/Resilience Measures

Under OFAC's Enforcement Guidelines, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response to an apparent violation of U.S. sanctions laws or regulations.

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.[14] This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.[15]

Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide,[16] will be

[13] 31 C.F.R. part 501, appx. A.
[14] To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The *Framework* is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.
[15] *See* FinCEN Guidance, FIN-2020-A006, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.
[16] *See* Cybersecurity and Infrastructure Security Agency Guidance, *Ransomware Guide*, September 2020, https://seculore.com/resources/cisa-ms-isac-publish-updated-ransomware-guide/

considered a significant mitigating factor in any OFAC enforcement response.[17] Such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others.

Cooperation with OFAC and Law Enforcement

Another factor that OFAC will consider under the Enforcement Guidelines is the reporting of ransomware attacks to appropriate U.S. government agencies and the nature and extent of a subject person's cooperation with OFAC, law enforcement, and other relevant agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed. In the case of ransomware payments that may have a sanctions nexus, OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response. OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.

While the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue to be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible. Victims should also report ransomware attacks and payments to Treasury's OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment. As noted, in doing so victims can receive significant mitigation from OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment.

17 *See* the U.S. government's website, https://www.cisa.gov/stopransomware, for additional guidance.

By reporting ransomware attacks as soon as possible, victims may also increase the likelihood of recovering access to their data through other means, such as alternative decryption tools, and in some circumstances may be able to recover some of the ransomware payment. Additionally, reporting ransomware attacks and payments provides critical information needed to track cyber actors, hold them accountable, and prevent or disrupt future attacks.

Contact Information for U.S. Department of Treasury Agencies:

- U.S. Department of the Treasury's Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
  - https://www.ic3.gov/default.aspx; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
  - https://secretservice.gov/contact/field-offices
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- Homeland Security Investigations Field Office
  - https://www.ice.gov/contact/

Ransomware Prevention Resources:

- U.S. Government StopRansomWare.gov Website
  - https://www.cisa.gov/stopransomware
- CISA Ransomware Guide
  - https://www.cisa.gov/stopransomware/ransomware-guide

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.