## 1. Overview

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) strongly encourages U.S. companies to employ a risk-based approach to sanctions compliance by developing, implementing and routinely updating a sanctions compliance program (SCP). This SCP is developed, implemented and maintained by COMPANY Inc. (COMPANY) to ensure compliance with U.S. economic and trade sanctions programs administered by OFAC. This SCP was created using recommendations, details and guidelines from documentation released from the U.S. Treasury: *A Framework for OFAC Compliance Commitments*[1] and *Economic Sanctions Enforcement Guidelines*[2].

## 2. Risk and Compliance Obligations

COMPANY Inc. has a low to moderate level of risk[3] attached to transactions with individuals within or attempting to enter the Contractor Workforce. The Contractor Workforce consists of Contract Workers: individuals who perform online work and earn virtual money on COMPANY's platform. Contract Workers may request payment through online payment providers such as Paypal. If a payment request is approved by COMPANY Administrators, money is withdrawn from a U.S. bank account and sent remotely to the Contract Worker. COMPANY and involved persons may be held liable if Administrators approve a transaction that violates an OFAC sanction, even if the violation is not obvious or unintentional. COMPANY must mitigate risk by appropriately screening and scrutinizing all Contract Workers, rejecting transactions, and reporting potential violations to the Workforce Management team and improving the guidelines of this SCP.

### 2.1 Low-Risk Contractors and Employees

Low-risk contractors and employees are typically developers, executives or consultants that reside in a low-risk country. Low-risk Contractors and Employees are exempt from Individual Screening Processes. It is the responsibility of the executive team to ensure a separate screening and monitoring process is in place for low-risk individuals.

Low-risk countries:

- United States of America
- Canada
- Mexico

---

[1] A Framework for OFAC Compliance Commitments https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

[2] Economic Sanctions Enforcement Guidelines https://www.treasury.gov/resource-center/sanctions/documents/fr74_57593.pdf

[3] Low to moderate level of risk is established using the FFIEC Bank Secrecy Act Anti-Money Laundering Examination Manual Risk Matrix and considering the automatic and robust compliance controls and systems in place, the compliance system's automatic adaptation to OFAC SDN List, record retention, and significant and responsive management involvement. https://www.treasury.gov/resource-center/sanctions/Documents/matrix.pdf

## 3. Maintenance and Administration

This SCP shall be circulated to all members of the COMPANY executive team. Any COMPANY employees or contractors working directly with Contract Workers or Payment Systems shall be provided a copy of this Policy in connection with their onboarding for review and it shall be part of training. The executive team and Workforce Management team are responsible for screening, overseeing the correct implementation of Payment Systems, record retention, and reporting as set forth herein.

The Workforce Management team is composed of COMPANY's Chief Executive Officer and Chief Technology Officer and any contractors or employees explicitly assigned to ensuring this SCP's compliance.

## 4. Sanction Programs

There are two types of sanctions under OFAC: Comprehensive Sanctions and Selective Sanctions. Comprehensive sanctions prohibit almost all trade and transactions with specific countries without a license from the U.S. government. COMPANY does not do business in countries where there are comprehensive sanctions. All transactions, directly or indirectly, involving Iran, Cuba, Sudan, Darfur, and Syria should be immediately cancelled or rejected. Additionally, if there is reason to believe that a transaction will eventually end up in one of these countries, the transaction should be cancelled or rejected.

Selective sanctions target individuals and entities that threaten international peace and stability, engage in violent acts, commit human rights violations, or support regimes that threaten U.S. interests, among other activities. Transactions may be approved in countries where country-based selective sanctions are in place provided the receiving Contract Worker has passed the Individual Screening Process, as detailed in Section 5.

Countries with Comprehensive Sanctions:

- Cuba
- Iran
- Syria
- Sudan and Darfur
- North Korea
- Crimea Region

Country-based Selective Sanctions:

- Balkans
- Belarus
- Burundi
- Central African Republic
- Democratic Republic of the Congo
- Iraq
- Lebanon
- Libya
- North Korea
- Somalia
- Russia
- Venezuela
- Yemen
- Zimbabwe
- Ukraine

Non-Country Based Specific Sanctions:

- Counter Terrorism
- Cyber-related
- Non-Proliferation Sanctions
- Rough Diamond Trade Controls
- Transnational Criminal Organizations
- Magnitsky Act Sanctions

OFAC maintains the Specially Designated Nationals and Blocked Persons List[4] and Consolidated Sanctions List[5], collectively the Sanctioned Persons and Entities Lists. These lists provide information to identify individuals or entities under a sanction program.

## 5. Individual Screening Process

A screening process is conducted for all Contract Workers prior to payment approval. The following Identifying Information should be solicited or automatically retrieved for each Contract Worker:

1. Written Name
2. Citizenship of Individual
3. Full Shipping Address
4. Photo of Government Identification Document containing Photo of individual
5. Internet Protocol Address (IP Address)

The following checks should be performed and documented:

1. The Written Name of the Identifying Information should match the name on the Photo of Government Identification Document.
2. The Full Shipping Address should not be within a country with Comprehensive Sanctions.
3. The Government Identification should not be expired.
4. The IP Address should not be within a country with Comprehensive Sanctions.
5. The Identifying Information does not match any person or entity on the Sanctioned Persons and Entities Lists. *See Section 5.1 for instructions on how to check for Sanctioned Persons.*

All Identifying Information should be stored and reproducible for reporting or auditing purposes.

Automatic systems or third-party solutions for identity verification may be used where the Workforce Management team has compelling reason to believe the solutions are highly accurate or less error-prone than manual human processes.

Contract Workers should be rescreened at the time of payment if the last screening was conducted more than 6 months from the time of the payment request. Identifying Information may be reused from the last screening period, provided they are not expired.

Individuals may use false or stolen Government Identification to circumvent the Individual Screening Process. The Workforce Management team should conduct audits on Contract Workers by verifying Identifying Information of suspicious or random individuals via a Video Chat.

Government Identification Documents include:

[4] Specially Designated Nationals And Blocked Persons List (SDN)Lists https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

[5] Consolidated Sanctions List https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

1. Any Identification issued from a valid Government Authority in the country, including drivers licenses and passports.
2. A United Nations Identification Card (UN Card).

Citizens of Venezuela must also comply with the requirements all Special Requirements for Venezuelan Citizens (Section 5.3).

Individuals may not have a shipping address or IP addresss location within the Crimea Region. Extra caution should be taken for citizens of Ukraine and Russia.

### 5.1 Searching for Sanctioned Persons

To search for a sanctioned person, the COMPANY Software System should be used. If the Software Systems identifies a matching individual, any transaction with individual should be rejected and future transactions with the individual should be denied. If the individual has had prior transactions with COMPANY, the OFAC Due Diligence[6] should be undertaken to confirm the individuals OFAC Name Match. If the name is a match, the OFAC Hotline should be contacted and the incident should be reported to the executive team.

### 5.2 Software System

The Software System should utilize the Sanctioned Persons and Entities Lists using fuzzy search techniques[7]. The accuracy of the programs should periodically be evaluated by the Workforce Management team and should remove 100% of sanctioned individuals that are input into it. Software Systems should update the Sanctioned Persons and Entities Lists on a monthly basis.

### 5.3 Special Requirements for Venezuelan Citizens

If the individual is located in Venezuela the individual must not be owned or controlled, directly or indirectly, by the government of Venezuela and must not have acted directly or indirectly for or on behalf of the Government of Venezuela or as a member of the Maduro regime. This check can be performed as follows:

1. The Contract Worker must sign an electronic document that they have not and do not have dealings with the Government of Venezuela, including the Central Bank of Venezuela and Petroleos de Venezuela, S.A. (PdVSA), or the Maduro regime.
2. The individual should not have any public dealings with the Government of Venezuela if the Contract Worker's name is searched on Google.
3. The individual should not have any public dealings with the Government of Venezuela in their employment history if the Contract Worker's profile is found on LinkedIn.

[6] OFAC Due Diligence is a recommended set of steps detailed by OFAC and can be found at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#match

[7] Fuzzy search techniques utilize approximate word matching and phonetic similarity to reveal more names than would normally appear in an exact name match search.

## 6. Pre-Payment Screening

Pre-Payment Screening should be conducted on any individual visiting a COMPANY website or application. It is the responsibility of the Workforce Management team to ensure that automated processes are in place to screen website visitors. The following checks should be put in place:

1. Any visitor from a comprehensively sanctioned country should not be able to view or access any COMPANY website.
2. Any visitor that reports their location as being from a comprehensively sanctioned country should be denied access to an account.

## 7. Additional Obligations

The Workforce Management team is responsible for the following tasks:

1. Upon learning of a weakness in internal controls pertaining to OFAC compliance, take immediate and effective action to implement compensating controls until the root cause of the weakness can be determined and remediated.
2. Make sure all relevant staff understand this SCP's policies and procedures.
3. Ensure that all auditing procedures have place at least once a year and are documented.
4. Ensure a culture of compliance by allowing anyone to report potential OFAC violations without repercussion, answering questions regarding compliance, ensuring any and all relevant parties are informed of additional requirements or obligations they may have, and ensuring that any relevant employees or contractors are knowledgeable of the latest version of this SCP.