LEGAL GUILD PLAYBOOK

AML Compliance and Due Diligence

INDEX

DISCLAIMER

NO ATTORNEY-CLIENT RELATIONSHIP OR LEGAL ADVICE: Communication of information by, in, to, or through this playbook and your receipt or use of it (1) is not provided in the course of and does not create or constitute an attorney-client relationship, (2) is not intended as a solicitation, (3) is not intended to convey or constitute legal advice, tax advice or financial advice and (4) is not a substitute for obtaining legal advice from a qualified attorney.

This Playbook was last modified in January 2022 and is subject to change according to new information and developing laws.

1. Overview of Playbook

This playbook is a collection of best practices and recommendations based on current NEAR ecosystem operations. It can serve as general guidance for Open Web Sandbox activity and other NEAR ecosystem initiatives.

Depending on your jurisdiction and activity, apart from being a best practice, it could be a legal obligation to fulfill **AML Compliance** and **Due Diligence** requirements detailed in this Playbook.

In the case of a DAO (Decentralized Autonomous Organization), it is essential to establish the governance structure and determine who is ultimately responsible for compliance matters (e.g., a specific DAO council, a user council, etc.). Disclosures in the code of the DAO or the technical specifications of a project proposal may help identify creators of a DAO.

Any questions, comments, or concerns you would prefer not to share publicly, please contact the Legal Guild (info@nearlegal.com)

2. AML Compliance

2.1 What is Compliance?

As an individual or organization, you may have to comply with many different regulations depending on your business model, customers, products, and operations jurisdiction as an individual or organization. The goal of those regulations and Compliance is to protect the integrity of the financial system and the customers and investors. It includes mainly Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regulations, sanctions regulations, consumer protection laws, data protection regulations, etc.

This document focuses on anti-money laundering and counter-terrorist financing regulations and sanctions regulations.

2.2 Why is AML Compliance important?

Compliance is important to:

1) Analyze vulnerability to money laundering and related risks
2) Establish minimum controls to mitigate risks
3) Comply with laws and regulations
4) Reduce operational and reputational risk

2.3 AML Compliance controls

AML Compliance controls include:

Controls to be set will depend on the jurisdiction where your business is located and on if it is fully decentralized or not. However, if your business is considered as a virtual asset service provider (VASP) or a financial intermediary, the following controls would apply:

- Registration and/or licensing with one or several regulators
- Application of a risk-based approach starting with a risk assessment
- Know Your Customer (KYC) on customers with different levels of controls depending on the risk; requirements here may vary from one jurisdiction to another. In some, it is only necessary to provide identity documents and selfies; in others, video identification is required, proof of address, and additional questions on the source of funds and purpose of the relationship.
- Sanctions screening
- Transaction monitoring which includes: AML transactions monitoring with classic red flags and specific crypto-related ones (deposit of crypto, conversion to private coins, conversion to fiat, withdrawal in a short period) and the use of blockchain analytics tools such as Chainalysis, TRM Labs, Merkle Sciences, CipherTrace, etc. which allows compliance officers to check the origin and destination of the virtual assets and their exposure to potential illegal activity:

    - Enhanced due diligence ("EDD")
    - Policies and procedures as well as governance
    - Trade surveillance (In the case of a crypto exchange)
    - Suspicious activity reporting
    - Record keeping
    - Training and awareness

2.4 Sanctions

Sanctions (economic and political sanctions) may apply to most businesses. Countries like Canada, the UK, US, and Switzerland and international organizations like the EU and the UN impose sanctions or other restrictive measures against nations, organizations, groups, industries, governments and entities controlled by governments, non-state entities, and individuals such as terrorist groups and terrorists, and list such entities, countries, groups, and individuals on sanctions lists.

Entities, countries, groups, and individuals on sanctions lists infringe internationally accepted behavior and norms, especially those identified as involved in weapons proliferation, as violators of human rights, or as involved in cybercrime.

Possibly you will deal with numerous individuals, corporations, business partners from various parts of the world. You must ensure these entities or persons are not sanctioned or subject to trade restrictions, such that business with them is either not permitted or subject to strict government controls.

You shall not directly or indirectly do business or enter into any transactions with sanctioned individuals/entities. It is why you should ask your customers and suppliers to provide information about their identity to comply with international and national sanctions regulations.

Consider checking against the following sanctions lists:

- Office of Foreign Assets Control (OFAC - US Department of the Treasury) economic and trade sanctions: https://sanctionssearch.ofac.treas.gov/
- United Nations (UN) Sanctions List: https://www.un.org/securitycouncil/content/un-sc-consolidated-list#individuals
- EU Financial sanctions List: https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions
- UK sanction lists: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

However, now you might be wondering how to comply as there are many different lists. The best choice is to work with a "sanction screening provider." In this case, you will either input your customer's name and date of birth manually in their software or use an API connection, and they will give you a result. If your customer's name matches the name of a sanctioned individual, you will need to investigate and determine if it is a proper match or a false positive. You are prohibited from opening a relationship if it is an appropriate match.

Currently, there is a free tool available online to check for sanctioned individuals on the above and other sanction lists with one search only: https://namescan.io/FreeSanctionsCheck.aspx

2.5 Customer Due Diligence

When engaging with third parties (natural or legal persons) and especially in financial services, it is important to be aware of your compliance and reputational risks. Compliance risks are primarily related to:

- Money laundering
- Terrorist Financing
- International sanctions
- Tax evasion
- Others (e.g., labor regulation, data protection, civil rights, etc.)

To limit the exposure to those risks, it is important to identify and gather information about the third parties you operate. Depending on which regulations you are subject to, the level of identification will differ.
In most jurisdictions, when providing financial services, you will be required to fully identify your customers, requiring them to provide identity documents, possibly proof of address, selfie, video identification, etc. This activity is called KYC (Know Your Customer/Counterparty). KYC is one part of the due diligence process called CDD (Customer Due Diligence or Counterparty Due Diligence).

In general, it is required to undertake CDD measures when:

(i) establishing business relations
(ii) carrying out occasional transactions above the applicable designated threshold (usually USD/EUR 10,000 or 15,000, the threshold is generally lower when it comes to virtual assets, e.g., USD 1,000)
(iii) there is a suspicion of money laundering or terrorist financing; or
(iv) there are doubts about the veracity or adequacy of previously obtained customer/counterparty identification data.

Each country may determine how it imposes specific CDD obligations, either through law or other enforceable means.

The CDD measures to be taken are as follows:

A. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information. This means that you will need to ask your customer to provide identity documents.

B. Identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity, such that one is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include understanding the ownership and control structure of the customer.

C. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

D. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout that relationship to ensure that the transactions being conducted are consistent with your knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds. It means doing transaction monitoring. For instance, you will need to determine red flags that trigger alerts.

The CDD measures to be applied normally depend on the level of risk of the client/counterparty. The level of risk per client will depend, for instance, on where the customer is located, which products they use, which means of payment are used, level of activities, etc.

To design your onboarding process, it is thus recommended to apply a Risk-Based Approach (RBA) which means that you will use different checks depending on the risk. For instance, if your customer is located in a high-risk country, you may want to require them to prove where the funds engaged are coming from. If they are located in a low-risk country, you may just need an identity check, etc. You may also want to tailor your onboarding framework depending on the funds deposited/traded.

3. Risk Level Classification

- Low risk: ⚠
- Medium risk: ⚠
- High risk: ⚠

Prohibited third-party ⚠ - Due to international sanctions and AML/CFT risks, the following third parties will not be accepted as counterparties:

a) Individuals or entities included in any of the official public sanctions lists of the United Nations, U.S.A. (OFAC), E.U or other countries

b) Persons of whom information is available, from which it can be inferred that they may be related to criminal activities, especially those allegedly associated with drug trafficking, organized crime, or terrorism

c) Persons who refuse to provide all or part of the information or documentation required or who, having provided it, refuse to provide a copy of their identification document

d) Persons who provide manifestly false documents or concerning whom there are serious doubts about their legality, legitimacy, or possible manipulation

e) Legal persons whose shareholders or control structure cannot be determined

In these cases, the business relationship will be refused/canceled, and the provision of services or granting any operation/rewards cannot be authorized.

High risk third-party ⚠ - Persons with one or more of the following characteristics, considered as risk elements, will be regarded as high-risk clients:

a) Those operations above a certain established (accumulated) amount of USD/EUR/equivalent (for example 10,000 USD/EUR/other)

b) Natural or legal persons whose nationality, domicile, or fiscal residence is in countries, territories, or jurisdictions considered to be high risk, including in any case those countries for which the Financial Action Task Force (FATF) requires the application of enhanced diligence measures (see Annex)

c) The business relationship or operation involves the transfer of funds from or to countries, territories, or jurisdictions considered to be high risk, in any case including those countries for which the Financial Action Task Force (FATF) requires the application of enhanced diligence measures (see Annex)

e) Individuals who are or have ties to Politically Exposed Persons (PEP)

f) Natural or legal persons acting through intermediaries

g) Any other natural or legal persons who, when analyzing their risk profile, present characteristics, due to their nature, their type of activity, the origin of the funds, or other relevant circumstances, which must be considered higher than normal risk

Any operation intended to be carried out with a high-risk counterparty requires preliminary analysis, enhanced due diligence, and the express approval of the DAO Council (or the council of users or similar established governance structure.).

Low risk third-party ⚠ - Persons with one or more of the following characteristics, considered as risk elements, will be regarded as regular risk clients:

a) Those operations with an (accumulated) amount of (virtual) currency more minor than a certain amount (for example, 10,000 USD/EUR/other)

b) Any counterparty or operation which is not considered a Prohibited third-party or High risk third-party.

If you're unclear about which level of risk applies to your client/counterparty, using the highest of the possible risk categories is recommended.

4. Further Guidance

4.1 Due Diligence levels

In general, the CDD measures must be applied to all clients/ counterparties. In case of high risk, additional third-party measures (enhanced due diligence or EDD) shall be used. Examples of EDD are:

- Obtaining other documentation (pay-slips, tax declarations, etc.) or clarifications from the counterparty
- Getting additional information about the counterparty through open-source intelligence (OSINT)
- Obtaining additional information on the customer and one beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds and source of wealth of the customer and, if applicable, the beneficial owner

- Obtaining information on the reasons for the intended or performed transaction
- Obtaining approval of the Senior Management for establishing or continuing the relationship
- Conducting enhanced monitoring of the business relationship
- Furthermore, as previously stated, an operation with a high-risk counterparty requires initial analysis and the express approval of the DAO Council (or the council of users or similar established governance structure.)
- For occasional transactions below a certain amount (for example, USD/EUR 1,000), it is generally allowed only to apply simplified due diligence, which means only identifying the counterparty. However, there is no occasional transaction as you will have a relationship with your customer most of the time.
- Simplified due diligence means that it is not necessary
- Verifying counterparty´s identity using reliable, independent source documents, data, or information
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that one is satisfied that it knows who the beneficial owner is
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout that relationship

Ongoing Due Diligence

Individuals and organizations should be required to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of third parties.

Suspicious Activity

Suspicious activity, in particular related to AML/CFT, should be investigated and, if necessary, reported to the local supervisor.
In case of sanctions risks, e.g., the counterparty/user is listed on sanctions lists, funds or other assets should be frozen (asset freeze). They should make an important report to the country's national responsible authority, which could entail a future confiscation.

Record Keeping

For at least five to ten years (depending on the jurisdiction), it is necessary to maintain all records required on CDD and domestic and international transactions to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit the reconstruction of individual transactions to provide, if necessary, evidence for the prosecution of criminal activity or other legal requirements

5. About this document

The content of this document is licensed under a Creative Commons license:

Attribution 4.0 International (CC BY 4.0)

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are accessible to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material
- for any purpose, even commercially.
- The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- Attribution - You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use

- No additional restrictions - You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.

- No warranties are given. The license may not give you all the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.

You may need to get additional permissions before using the material as you intend.

SANTIAGO CHAMAT

Executive Director

EDO BAKKER

Team Core

Annex: High-risk and other monitored jurisdictions

A. High-Risk Jurisdictions:

- Democratic People's Republic of Korea (DPRK)
- Iran

B. Jurisdictions with strategic deficiencies:

- Albania
- Barbados
- Burkina Faso
- Cambodia
- Cayman Islands
- Haiti
- Jamaica
- Jordan
- Mali
- Malta
- Morocco
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Philippines
- Senegal
- South Sudan
- Syria
- Turkey
- Uganda
- Yemen
- Zimbabwe