

# AML Risk Report

Report Generation Block  
Mode: Personal

USFG,  
100 F Street, NE,  
Washington, DC 20549,  
USA



\*where 100% reflects low-risk funds, and 0% reflects illicit funds

**Scan result:** As a result of the conducted review, it has been determined that the wallet has an AML rating of over 50%. This rating is acceptable and should not raise any suspicions. However, in certain cases, justified protective measures may be implemented to prevent any illegal activities. Next, you will be able to review the criteria used for the verification process.

Please note that according to company policy, we cannot disclose the reasons why your wallet does not have a 100% AML rating, as the information obtained could be used for illegal purposes. Rest assured, your rating is still within acceptable limits.

If you have any additional questions or need clarification, you can always contact our technical support specialists, who will be happy to answer all your questions. We would like to remind you that you will soon be able to review the criteria used for the verification process, as well as read the disclaimer.



# AML Identifies 26 Money Laundering Risk Sources:

## Danger

### ● **Child Exploitation**

Persons associated with child exploitation.

### ● **Dark Market**

Coins associated with illegal activities.

### ● **Dark Service**

Coins related to child abuse, terrorist financing or drug trafficking.

### ● **Enforcement action**

The entity is subject to proceedings with legal authorities.

### ● **Fraudulent Exchange**

Exchanges involved in exit scams, illegal behavior, or whose funds have been confiscated by government authorities.

### ● **Gambling**

Coins associated with unlicensed online games.

### ● **Illegal Service**

Coins associated with illegal activities.

### ● **Mixer**

Coins that passed through a mixer to make tracking difficult or impossible. Mixers are mainly used for money laundering.

### ● **Ransom**

Coins obtained through extortion or blackmail.

### ● **Sanctions**

Sanctioned entities.

### ● **Scam**

Coins that were obtained by deception.

## ● **Stolen Coins**

Coins obtained by hijacking someone else's cryptocurrency.

## ● **Terrorism Financing**

Entities associated with terrorism financing.

## **Suspicious sources**

### ● **ATM**

Coins obtained via cryptocurrency ATM operator.

### ● **Exchange | High Risk**

An entity becomes high-risk based on the following criteria:

**No KYC:** Requires absolutely no customer information before allowing any level of deposit/withdrawal, or makes no attempt to verify that information.

**Criminal Connections:** Criminal charges against the legal entity in connection with AML/CFT violations.

**Impact:** High exposure to risky services such as darknet markets, other high-risk exchanges, or blending is defined as a service whose direct high-risk exposure differs by one standard deviation from the average of all identified exchanges over a 12-month period.

**Jurisdiction:** based in a jurisdiction with weak AML/CFT measures.

**Unlicensed:** Does not have any specific license to trade cryptocurrencies.

### ● **P2P Exchange | High Risk**

The organization does not have any special license to conduct business related to the provision of cryptocurrency exchange services, when participants exchange directly with each other, without intermediaries.

It also includes entities that are licensed but located in listed jurisdictions, are listed as non-cooperating companies by the FATF, or do not provide KYC for large-value transactions, making them attractive for money laundering.

## Trusted sources

### ● Exchange

The organization allows users to buy, sell and trade cryptocurrencies by holding trading licenses that include the following aspects of the services:

— Depository, brokerage or other related financial services that provide exchange services where participants interact with a central party.

And does not include:

— Licenses for non-specific financial services and jurisdictions included in the FATF non cooperative list.

They represent the most important and most used category of entities in the cryptocurrency industry, accounting for 90% of all funds sent through these services.

### ● ICO

The organization that crowdfunds its project by selling their newly minted cryptocurrency to investors in exchange for fiat currency or more common cryptocurrencies such as Bitcoin and Ether.

There are many legitimate examples of these offerings, but also many cases where bad actors raise funds through ICOs, then they take the money and disappear.

### ● Marketplace

Coins that were used to pay for legal activities

### ● Merchant Services

The entity that allows businesses to accept payments from their customers, also known as payment gateways or payment processors.

It often facilitates conversions to local fiat currency and clearing the funds into the merchant's bank account.

### ● Miner

Coins mined by miners and not forwarded yet.

### ● Other

Coins obtained through airdrops, token sales or other means.

### ● P2P Exchange

The entity is licensed to conduct a business that is specific to providing cryptocurrency exchange services where participants exchange directly with each other, without a middleman.

It does not include non-specific financial services licenses and jurisdictions that are on the non cooperative FATF list.

 **Payment Processor**

Coins associated with payment services.

 **Seized Assets**

Crypto assets seized by the government.

 **Wallet**

Coins stored in verified wallets.

## Disclaimer

AML takes all steps necessary to provide an independent, up-to-date analysis and accurate information in the Report.

AML is not liable for any changes in assumptions and updates to this report in case of new facts or circumstances occurring after the date of the Report or facts that were not known to AML at the time of generation of this Report.

Any decision taken by the recipient of this Report is made solely on their own risk. The liability of AML is hereby excluded to the fullest extent permitted by the applicable law.

The Report does not discharge any obligation of proper internal risk assessment and/or decision making process. Certain information, due to high risk (e.g. crime related), used for analysis, may not be able to be disclosed to the recipient.

In cases of increased risk, user coins may be temporarily frozen in certain situations until the circumstances are clarified.

To the fullest extent permitted by applicable law, in no event will AML services, or any of its respective service providers, have any liability arising from or related to your use of or inability to use the services for:

a) any act or alleged act, or any omission or alleged omission, that does not constitute wilful misconduct by AML, as determined in a final, non-appealable

judgment by a court of competent jurisdiction;

b) lost profits, cost of substitute goods or services, loss of data, loss of goodwill, business interruption, computer failure or malfunction or any other consequential, incidental, indirect, exemplary, special or punitive damages;

c) direct damages in amounts that in the aggregate exceed the amount actually paid by you for the services;

d) any third-party claims (whether based in statute, contract, tort or otherwise).

The foregoing limitations:

a) will apply whether such damages arise out of breach of contract, tort (including negligence) or otherwise and regardless of whether such damages were foreseeable or AML was advised of the possibility of such damages; and

b) include any loss caused by the failure of the services to correctly identify participants in blockchain transactions or the levels of any associated risks such as fraudulent activity, and you acknowledge.