Company Disclosures:

At MaskEX, we are committed to provide our clients with comprehensive information about the material risks associated with Virtual Assets. It is essential for our clients to have a clear understanding of these risks before engaging in Virtual Asset activities. Please take note of the following key points:

A. DISCLAIMER

Virtual Assets, including but not limited to cryptocurrencies, may lose their value in part or in full. These assets are subject to extreme price volatility, which means their values can fluctuate significantly over short periods.

B. RISK DISCLOSURE STATEMENT

At MaskEX, we believe in transparency and want to ensure that our users are fully aware of the potential risks associated with Virtual Assets. It is essential for our clients to have a clear understanding of these risks before engaging in Virtual Asset activities. Please take note of the following key points:

i. Value Volatility and Loss:

a) Volatility: Virtual Assets can experience extreme price fluctuations, which means they can rapidly increase or decrease in value.

b) Potential Loss: There is a risk that Virtual Assets may lose their value in part or in full. Investors should be aware that their investments can decrease significantly or become worthless.

ii) Transferability and Irreversibility:

a) Transfer Limitations: Virtual Assets may not always be transferable. There might be instances where transferring assets is restricted or not possible.

b) Irreversible Transfers: Some Virtual Asset transfers are irreversible. Once a transaction is made, it cannot be undone, and any incorrect transfers may result in permanent loss of assets.

iii. Liquidity Concerns:

a) Liquidity Risk: Virtual Assets may not always be liquid. This means that there might be limited opportunities to buy or sell these assets quickly without affecting their price.

iv. Privacy and Public Records:

a) Non-Private Transactions: Some transactions involving Virtual Assets are not private and may be publicly recorded on Distributed Ledger Technologies (DLTs), such as blockchain. This means that transaction details could be accessible to the public and could potentially compromise user privacy.

v. Fraud, Manipulation, and Theft:

a) Fraud and Manipulation: Virtual Assets may be subject to fraudulent schemes or manipulation, affecting their value and integrity.

b) Theft and Hacks: There is a risk of Virtual Assets being stolen through hacks or other targeted schemes. Unlike traditional assets, Virtual Assets may not benefit from legal protections or insurance coverage, making recovery difficult in case of theft. It's important to note that Virtual Assets may not benefit from the same legal protections as traditional assets, potentially leaving you with limited recourse in case of loss.

We strongly advise all clients to conduct thorough research and seek professional advice before engaging in Virtual Asset transactions. Understanding these material risks is crucial for making informed decisions and managing your exposure to potential financial losses.

MaskEX is dedicated to transparency and client education. If you have any questions or require further information about Virtual Asset risks, please do not hesitate to contact our support team at support@maskex.com or refer to our educational resources. Your financial well-being is our top priority, and we are here to assist you every step of the way.

C. CONFLICT OF INTEREST DISCLOSURE

We are committed to transparency and integrity in our operations. To ensure that our clients are well-informed about any potential conflicts of interest, we provide the following detailed description:

i. Nature of Conflicts

We acknowledge that conflicts of interest may arise in the course of our activities. These conflicts could result from various factors, including but not limited to, our relationships with other entities, financial interests, or the provision of services to multiple parties with differing interests.

ii. Management of Conflicts

We have implemented comprehensive policies and procedures to identify, manage, and mitigate conflicts of interest. Our approach includes regular assessments, employee training, and appropriate measures to ensure fair and unbiased decision-making.

iii. Disclosure of Specific Conflicts

Any actual or potential conflicts of interest related to our activities are disclosed in a timely manner. This disclosure includes information on the nature of the conflict, parties involved, and the steps taken to address and manage the conflict to safeguard the interests of our clients.

D. WHISTLEBLOWING POLICY

We are committed to maintaining the highest standards of ethics, integrity, and transparency. Our whistleblowing policy is designed to encourage and facilitate the reporting of any concerns related to unethical behavior, violations of laws or regulations, or any other activities that may pose a risk to the integrity of our operations. We believe in fostering a culture where individuals feel empowered to speak up without fear of retaliation.

i. Reporting Mechanism

Individuals/Employees can report concerns through our dedicated whistleblowing channels available in the Company Handbook. Reports can be made anonymously if the whistleblower wishes to remain unidentified. However, providing contact information is encouraged to facilitate further investigation.

ii. Protection for Whistleblowers

We strictly prohibit retaliation against whistleblowers. Any employee found to be engaging in such behavior will be subject to disciplinary action. Whistleblowers' identities will be kept confidential to the extent permitted by law, and only disclosed on a need-to-know basis for the purpose of investigation.

iii. Investigation Process

Reports will be promptly and thoroughly investigated by our designated whistleblowing team. The outcome of investigations will be communicated to the whistleblower within a reasonable timeframe, considering the complexity of the matter.

iv. Non-Retaliation Assurance

We are committed to creating an environment where individuals can report concerns without fear of adverse consequences. Any employee found to have retaliated against a whistleblower will face disciplinary action, up to and including termination. We encourage all stakeholders, including employees, clients, and other partners, to come forward with any concerns they may have. Your commitment to upholding our shared values is essential in maintaining the integrity of our services.

E. ANTI BRIBERY POLICY

We adhere to a zero-tolerance approach towards bribery and corruption. Our commitment to integrity is unwavering, and we maintain strict ethical standards in all aspects of our business operations. Your trust is paramount, and we are dedicated to fostering a transparent and responsible business environment”

i. ABC Governance

We are committed to conducting business ethically and in compliance with all applicable laws and regulations related to the prevention of bribery and corruption. Our Anti-Bribery & Corruption (ABC) team is responsible for overseeing the implementation of this policy and ensuring that appropriate measures are in place to prevent, detect, and report instances of bribery and corruption.

ii. ABC Guidelines and Tolerance

We maintain a zero-tolerance approach towards bribery and corruption in all its forms, both direct and indirect. All employees, directors, officers, and associated entities are expected to adhere to this policy and to report any actual or suspected instances of bribery or corruption to the appropriate authorities.

iii. Consequences of Policy Breach

Breaches of this policy may result in disciplinary action, up to and including termination of employment or contractual relationships. Additionally, individuals involved in bribery or corruption may face legal consequences, including criminal prosecution and civil liabilities.

iv. Policy on Payments, Gifts, and Hospitality (Including through Associated Entities)

It is prohibited for any of the Company, members of the Board and all Staff, to— give, promise to give, or offer, a payment, gift or hospitality to a third party or otherwise engage in or permit a bribery offence to occur, with the expectation or hope that an advantage in business will be received or to reward a business advantage already given;

give, promise to give, or offer, a payment, gift or hospitality to a third party to facilitate or expedite a routine procedure;

accept a payment, gift or hospitality from a third party if it knows or suspects that such payment, gift or hospitality is offered or provided with an expectation that a business advantage will be provided by the Company in return;

threaten or retaliate against another member of the Board or Staff who has refused to commit a bribery offence or who has raised concerns; and

engage in any activity that might lead to a breach of the anti-bribery and corruption of the relevant laws.

F. DATA PRIVACY POLICY

We are committed to safeguarding the privacy and security of your data. Our data privacy policy is designed to provide transparency about the personal information we collect, how it is used, and the measures we take to protect it.

Mask Virtual Assets exchange LLC is ISO/IEC 27001:2022 certified, adhering to internationally recognized standards for information security management. Our certification ensures that we have implemented robust processes to protect the confidentiality, integrity, and availability of sensitive information. However, while we strive to maintain the highest security standards, no system is completely immune to risks. Users are encouraged to follow best security practices to safeguard their own accounts and information.

i. Collection and Use of Personal Information

We collect personal information from users when they engage with our platform or services. This may include, but is not limited to, information provided during account registration, transaction processing, and communication with our support team. The information collected is used for account management, service improvement, and to comply with regulatory requirements.

ii. Data Protection Measures

We implement robust technical and organizational measures to secure your personal data. This includes encryption, access controls, and regular security audits. We continuously strive to enhance our security protocols to protect your information from unauthorized access or disclosure.

iii. Sharing of Information:

We do not sell or share your personal information with third parties for their marketing purposes. Your data may be shared with trusted third-party service providers for purposes such as payment processing or compliance with legal obligations.

iv. Your Rights:

You have the right to access, correct, or delete your personal information held by us. To exercise these rights or inquire about our data practices, please contact us through the provided channels.

F. VA Standards

MaskEX is committed to maintaining high standards for all Virtual Assets involved in our VA Activities. To this end, we have established comprehensive VA Standards, ensuring due diligence and compliance with applicable laws and regulations.

1. Description of VA Standards i. Security Measures

a) **Encryption:** All user data and transaction information are encrypted using industrystandard protocols to ensure data security and integrity.

b) **Two-Factor Authentication (2FA):** We implement 2FA to provide an additional layer of security for user accounts.

c) **Cold Storage:** A significant portion of users' virtual assets are stored in cold wallets, which are offline and less vulnerable to hacking.

ii. Compliance with Anti-Money Laundering (AML) Regulations

MaskEX adheres to strict AML policies to prevent money laundering and terrorist financing. This includes the identification and reporting of suspicious activities.

a) Transaction Monitoring: Continuous monitoring of transactions is conducted to detect and report any unusual or suspicious activities.

iii. Customer Verification Procedures

a) Know Your Customer (KYC): We follow robust KYC procedures to verify the identity of our customers. This includes collecting and verifying personal information and documentation.

b) **Enhanced Due Diligence (EDD):** For higher-risk customers, we perform EDD to gain a better understanding of their financial activities and mitigate potential risks. C) For comprehensive guidelines and standards that MaskEX adheres to in its operations for KYC Verification, please follow Know Your Customer (KYC)

iv. Transaction Monitoring

MaskEx is committed to have continuous monitoring of transactions is conducted to detect and report any unusual or suspicious activities.

a) Real-Time Monitoring: Transactions are monitored in real-time to ensure compliance with regulatory requirements and to detect any potentially illicit activities.

b) Automated Alerts: Our systems generate automated alerts for any transactions that deviate from normal patterns, enabling us to investigate and take appropriate actions promptly.

v. Operational Policies

a) Internal Controls: We have robust internal controls in place to manage risks and ensure the integrity of our operations.

b) Privacy Policies: User privacy is a priority, and we adhere to strict privacy policies to protect personal data.

c) Incident Response: In the event of a security breach or other incidents, we have a comprehensive incident response plan to mitigate the impact and prevent future occurrences.

d) For detailed information on our AML/CFT policy, users can refer to the MaskEX AML/CFT Policy.

This link provides comprehensive guidelines and standards that MaskEX adheres to in its operations AML-CFT Policy

2. Legal and Regulatory Compliance

Statement of Compliance with Laws and Regulations

i. Local and International Laws

a) **Compliance with UAE Laws:** MaskEX complies with all relevant local laws and regulations in the UAE, including those issued by the Virtual Assets Regulatory Authority (VARA).

b) Global Regulatory Frameworks: We also adhere to international standards and guidelines to ensure global regulatory compliance.

ii. Regulatory Frameworks and Guidelines:

a) VARA Rulebook: We follow the guidelines and frameworks issued by VARA, which govern the operation and regulation of virtual assets.

b) AML and KYC Compliance: We comply with global AML and KYC standards to prevent money laundering and ensure the integrity of our financial system.

c) For detailed information on our regulatory compliance,This link provides comprehensive guidelines and standards that MaskEX adheres to in its operations.VARA Rulebook

MaskEX is dedicated to providing a secure and compliant trading environment by adhering to these standards. We continuously update our VA Standards to adapt to changes in the Virtual Asset landscape and regulatory requirements.

We may update our privacy policy to reflect changes in regulations or our business practices. Any modifications will be communicated through our website, and we recommend reviewing the policy periodically.