Veritas Cryptoasset Risk Disclosure

Cryptoassets are highly volatile and their value can fluctuate. Veritas is not liable for any losses that you suffer while staking your assets, as a result of any incident that is not attributable to us, including due to price fluctuation of cryptoassets or a Protocol or other network upgrade or failure.

To make sure you understand risks linked with crypto, by accessing to your Veritas Crypto Account you agree to accept risks below.

1. Risk of Total Loss

- The value of cryptoassets is highly volatile and can decrease as quickly as it may increase. Pricing is often determined in opaque markets, without centralized oversight. Be prepared for the possibility of losing your entire investment.
- Your cryptoassets may be lost due to security breaches, criminal activity, or the failure of service providers.
- Participating in staking involves "slashing" risk — this refers to potential penalties (partial or total asset loss) if validators act dishonestly or fail to meet protocol standards.

2. Limited Regulatory Protections

- Investments in cryptoassets are not covered by most investor protection schemes, such as the Investor Compensation Fund (ICF). This means your funds are not safeguarded in the event of firm insolvency or misconduct.
- Additionally, complaints made against cryptoasset service providers typically fall outside the jurisdiction of financial ombudsman bodies.

3. Liquidity Risks

- You may not be able to sell your cryptoassets when desired. Market conditions, such as low demand or limited trading volume, can make it difficult to liquidate positions without incurring significant losses.
- Technical failures, including system outages or cyberattacks, may temporarily prevent access to platforms or delay transactions.
- Some staking mechanisms enforce lock-up periods during which assets cannot be withdrawn or sold.

4. Fraud and Security Threats

- The crypto space is often targeted by fraudulent schemes — phishing, fake investment opportunities, or malicious actors impersonating legitimate services.
- While we apply strict security protocols to protect users, no platform can guarantee absolute protection. Exercise caution, verify sources, and report suspicious activity to our support team immediately.

5. Product Complexity

- Cryptoasset-related investments can be complex and may not be easily understood without sufficient research.
- Before engaging, ask yourself:
    - Can I afford to lose the full amount I invest?
    - Do I understand how the cryptoasset or product works?
    - Am I capable of securely managing the devices and accounts used to store or transfer these assets?

6. Diversification is Essential

- Concentrating all your capital in one type of investment increases exposure to loss. Spreading investments across multiple asset types can reduce overall risk.
- As a general principle: never invest more than you are willing — or can afford — to lose.

7. Specific Risks by Asset Type

A. Staking Assets

Assets like ETH or DOT used for staking present specific risks:

- **Slashing**: Losses may occur if validators breach protocol rules.
- **Liquidity Risk**: Lock-up periods can delay access to staked funds.
- **Variable Rewards**: Yields are subject to change and not guaranteed.
- **Consensus Changes**: Updates to network validation mechanisms may introduce new vulnerabilities.

B. Stablecoins

Assets pegged to fiat currencies or other reserves (e.g., USDT, USDC) carry distinct risks:

- **Collateral Risk**: Volatility in underlying reserves may affect price stability.
- **Redemption Risk**: Redeeming stablecoins may be difficult during high-stress market events.
- **Foreign Exchange Risk**: Exposure to USD-based assets may result in exchange rate losses.
- **Counterparty Risk**: Third-party reserve managers may fail to maintain sufficient collateral.

C. DeFi Tokens

Tokens linked to decentralized finance protocols (e.g., AAVE) include risks such as:

- **Smart Contract Exploits**: Vulnerabilities may lead to loss of funds.
- **Scams**: Some projects are created solely to defraud investors.
- **Data Dependency**: Protocols reliant on external data can be disrupted or manipulated.
- **Complexity**: Understanding DeFi systems requires technical literacy.

D. Wrapped Tokens

Wrapped assets (e.g., wAXL) that represent tokens from other blockchains may expose you to:

- **Collateral Insufficiency**: Lack of proper backing may devalue the asset.
- **Custodial Risk**: Losses may occur if third-party custodians suffer breaches or go bankrupt.
- **Smart Contract Risk**: Code bugs may be exploited.
- **Bridge Vulnerabilities**: Technical flaws in cross-chain bridges can interrupt transfers.
- **Price Divergence**: Market shocks may cause decoupling from the underlying asset's value.

E. Meme Tokens

Tokens driven by internet trends (e.g., DOGE) are especially risky:

- **High Volatility**: Prices may swing wildly due to sentiment, hype, or social media trends.
- **Market Manipulation**: These assets are prone to pump-and-dump schemes.
- **Lack of Transparency**: Project details and leadership are often unclear.
- **Emotional Investing**: Decisions based on hype can result in rapid and significant losses.