PUBLIC

Risk Disclosures Standard Chartered Luxembourg

1. PURPOSE AND SCOPE

Standard Chartered Luxembourg S.A. ("**SCL**" or the "**Company**") is committed to providing secure crypto-asset custody services to its clients. In connection with the provisions of such services, SCL recognises that the offered services might expose clients to several risks.

The purpose is to provide clients with an overview of the principal risks associated with SCL' crypto-asset custody services. The risks described below are not an exhaustive list and are intended to highlight certain key risks that clients should consider when using the services provided by the Company.

2. RISKS

The risks associated with crypto-assets custody include - but are not limited to - the following:

2.1 Regulatory Risk

The legal, regulatory and supervisory framework applicable to crypto-assets custody services continues to evolve and may be subject to significant changes.

Changes in applicable laws, regulations, regulatory guidance, may materially affect SCL's crypto-asset custody activities, the manner in which services are provided, or the availability of certain crypto-assets or related services.

Regulatory developments may also result in additional requirements, restrictions, limitations or costs being imposed on SCL or its clients.

SCL monitors relevant legal and regulatory developments and maintains processes designed to ensure that its crypto-asset custody activities remain compliant with applicable laws and regulations. However, SCL cannot guarantee that future regulatory or legal developments will not adversely affect the availability, functionality or continuity of particular services.

2.2 Blockchain and crypto-asset Risk

Crypto-assets rely on distributed ledger technology, blockchain protocols, cryptographic systems and network participants that may be subject to vulnerabilities, defects, failures or malicious attacks.

Risks may include, without limitation:

- software bugs, coding errors or protocol vulnerabilities;
- blockchain reorganisations, forks or changes to network governance;
- consensus failures, network congestion or transaction delays;
- double-spending attacks, 51% attacks or other attacks against blockchain networks;
- smart contract vulnerabilities or failures;
- technological developments that may reduce the effectiveness of existing cryptographic protections; and
- actions or decisions taken by protocol developers, validators, issuers or governance participants that may adversely affect a crypto-asset.

Transactions recorded on a blockchain are generally irreversible. Once confirmed, transactions may not be capable of cancellation, reversal or recovery, including in cases of error, fraud or unauthorised activity.

2.3 ICT and Cybersecurity Risk

The custody and administration of clients' crypto-assets are exposed to a range of information and communication technology ("**ICT**"), cybersecurity, operational and security risks throughout the lifecycle of the crypto-assets.

Such events may include systems disruptions, natural disasters, act of terrorism, cyber-attacks, exploitation of software vulnerabilities, attacks against blockchain protocols, telecommunications failures, human error, infrastructure outages or disruptions affecting third-party service providers, civil unrest or other extraordinary circumstances.

SCL maintains an ICT and cybersecurity risk management framework designed to identify, assess, monitor and mitigate such risks through governance arrangements, security controls, operational procedures, testing and ongoing oversight.

SCL maintains business continuity, disaster recovery and operational resilience arrangements designed to support the continuation and recovery of critical services.

Cybersecurity incidents, operational failures or technology disruptions may occur and could result in service interruptions, delays, loss of data, unauthorised transactions, loss of access to crypto-assets or, in certain circumstances, the loss of crypto-assets.

2.4 Third-Party Risk

The provision of crypto-asset custody services may involve reliance on third-party service providers, including technology providers, telecommunications providers, cloud service providers, market infrastructure providers and other external service providers.

Failures, disruptions, insolvencies, cyber incidents or operational deficiencies affecting such third parties may adversely impact the availability, security or performance of custody services.

Although SCL conducts oversight of its service providers, it cannot eliminate all risks arising from third-party relationships.

2.5 Fraud Risk

Crypto-asset custody services may be exposed to fraud risks arising from external fraudsters, cybercriminals, organised criminal groups, malicious insiders, compromised accounts, social engineering attacks or other fraudulent activity.

Fraud may include, without limitation, phishing attacks, impersonation, business email compromise, identity theft, fraudulent instructions, account takeover, manipulation of wallet addresses, social engineering, insider misconduct and the misuse of compromised credentials or wallets. Fraudulent activity may result in unauthorised transactions, theft, loss or misappropriation of crypto-assets.

SCL maintains controls designed to prevent, detect and respond to fraudulent activity. However, no control framework can eliminate all fraud risks and losses may occur notwithstanding the implementation of reasonable safeguards.

Clients should remain vigilant and exercise caution in relation to unsolicited communications, requests for credentials, changes to wallet addresses, urgent transaction requests and communications purporting to originate from SCL or another trusted party.

Crypto-assets involve significant risks and clients may lose some or all of the value of their crypto-assets. SCL therefore encourages all clients to carefully consider these risks before engaging in crypto-asset custody services.