Global Cryptoasset Standards

Foreword

I. What Is the Global Cryptoasset Standards?

This set of global principles of good practice in the Global Cryptoasset Standards has been developed to provide a common set of guidelines to promote the integrity and effective functioning of the Cryptoasset Market. It is intended to promote a robust, fair, liquid, open, and appropriately transparent market in which a diverse set of Market Participants, supported by resilient infrastructure, are able to confidently and effectively transact at competitive prices that reflect available market information and in a manner that conforms to acceptable standards of behavior.

As made clear by market events in the Cryptoasset industry, there is a need amongst Market Participants for Cryptoasset Standards which define principles of good practice. The industry and engaged consumers would benefit from Market Participants adhering to standards for matters including ethics, governance, and risk mitigation, as this would facilitate responsible activity and potentially reduce instances of institutional collapse. There are many unique features of the Cryptoasset industry to consider as compared to the traditional finance industry, so Market Participants, such as those who drafted these Cryptoasset Standards, are particularly well positioned to provide this guidance. The Global Cryptoasset Standards does not impose legal or regulatory obligations on Market Participants nor does it substitute for regulation, but rather it is intended to serve as a supplement to any and all local laws, rules, and regulation by identifying global good practices and processes.

The Global Cryptoasset Standards is maintained by the Global Digital Finance (GDF).

The GDF is an industry association accelerating digital finance through the adoption of best practices and standards and engagement with regulators and policymakers. Established in 2018, GDF has convened a broad range of industry participants, with 300+ global community members – including some of the most influential companies, academics and professional services firms supporting the industry. The Global Cryptoasset Standards effort was specifically the focus of the GDF's Global Financial Institutions Crypto Working Group (GFIC), which is chaired by Standard Chartered and Ownera. The GFIC consists of diverse members of the crypto ecosystem including banks, asset managers, exchanges, securities depositories, virtual asset service providers, law firms, and industry associations.

The GDF assesses regularly whether particular Cryptoasset Market developments warrant specific revisions to the Global Cryptoasset Standards and when judged appropriate, undertakes a comprehensive review of the Global Cryptoasset Standards.

The GDF has leveraged the framework and high-level principles existing in the FX Global Code to define the framework for the Global Cryptoasset Standards. The GDF received explicit approval to consider the FX Global Code in this drafting process. In certain instances, the Global Cryptoasset Standards includes principles referenced in the FX Global Code without material revision, as they are directly analogous, applicable, and appropriate in a Cryptoasset context. In other instances, the GDF makes substantive revisions to principles in the FX Global Code to address risks specific to Cryptoasset Markets. Finally, the GDF established a number of net new principles to provide guidance for unique risks in the Cryptoasset Markets.

More information on the GDF is available at www.gdf.io.

The Global Cryptoasset Standards is organized around six leading principles:

- Ethics: Market Participants are expected to behave in an ethical and professional manner to promote the fairness and integrity of the Cryptoasset Market.
- Governance: Market Participants are expected to have a sound and effective governance framework to provide for clear responsibility for and comprehensive oversight of their Cryptoasset Market activity and to promote responsible engagement in the Cryptoasset Market.
- Execution: Market Participants are expected to exercise care when negotiating and executing transactions in order to promote a robust, fair, open, liquid, and appropriately transparent Cryptoasset Market.
- Information Sharing: Market Participants are expected to be clear and accurate in their communications and to protect Confidential Information to promote effective communication that supports a robust, fair, open, liquid, and appropriately transparent Cryptoasset Market.
- Risk Management and Compliance: Market Participants are expected to promote and maintain a robust control and compliance environment to effectively identify, manage, and report on the risks associated with their engagement in the Cryptoasset Market.
- Confirmation and Settlement Processes: Market Participants are expected to put in place robust, efficient, transparent, and risk-mitigating post-trade processes to promote the predictable, smooth, and timely settlement of transactions in the Cryptoasset Market.

The Global Cryptoasset Standards and Applicable Law

Market Participants must be aware of, and comply with, the laws, rules, and regulations applicable to them and the Cryptoasset Market in each jurisdiction in which they do business (Applicable Law). Market Participants remain responsible for having internal policies and procedures in place that are designed to comply with such Applicable Law.

The content of this guidance in no way supplants or modifies Applicable Law. Similarly, this guidance does not represent the judgement nor is it intended to bind the discretion of any regulator, supervisor, or other official sector entities with responsibility over the relevant markets or Market Participants, and it does not provide a legal defense to a violation of Applicable Law.

The Global Cryptoasset Standards should serve as an essential reference for Market Participants when conducting business in the Cryptoasset Market and when developing and reviewing internal procedures. It is not intended to be a comprehensive guide to doing business in the Cryptoasset Market.

Certain terms used in this Global Cryptoasset Standards may have specific definitions or meanings under Applicable Law, which may imply certain duties or obligations in a jurisdiction. Since this document is meant to serve as a code of good practice for Market Participants operating in different jurisdictions, it is not intended that the local meaning of terms in any one jurisdiction apply to the interpretation of the Global Cryptoasset Standards. For the avoidance of doubt, terms used in this Global Cryptoasset Standards should be read according to their commonly accepted meaning as terms of market practice in the Cryptoasset Market, and no specific legal or regulatory meaning should be imputed or ascribed to them.

Annex 2 contains a glossary of the capitalized terms featured throughout the Global Cryptoasset Standards*.*

II. To Whom Do the Global Cryptoasset Standards Apply?

The Cryptoasset Market features a diverse set of participants who engage in the market in different ways and across various Cryptoasset products. The Global Cryptoasset Standards is written with this diversity in mind, however, it is expected to apply specifically to Cryptoasset Market Participants that engage in the Cryptoasset Market, including sell-side and buy-side entities, liquidity providers, operators of Cryptoasset Trading Venues, and other centralized entities providing brokerage, execution, and settlement services. Given the diversity and rapidly evolving nature of the Cryptoasset industry, there can be no universal "one size fits all" set of standards, however the Global Cryptoasset Standards is intended to serve as a guiding example of a common set of principles for responsible participation in the market.

For the purposes of this document, a "Market Participant[1]" is a person or organization (regardless of legal form) that:

i. is active in Cryptoasset Market as a regular part of its business and is engaged in the activity of the purchase or sale of Cryptoassets, or in transactions designed to result in gains or losses based upon the change in one or more Cryptoasset prices, such as derivatives, whether deliverable or non-deliverable, either directly or indirectly through other Market Participants; or
ii. operates a facility, system, platform, or organization through which participants have the ability to execute the type of transactions described in (i); or
iii. provides Cryptoasset benchmark execution services; and
iv. is not considered a retail market participant in the relevant jurisdiction(s).

The term includes any personnel who conduct the foregoing on behalf of a Market Participant.

As a guide, the following types of persons or organizations would generally be expected to engage in Cryptoasset Market activities as Market Participants, as described in (i) – (iv) above:

- financial institutions;
- central banks, except where this would inhibit the discharge of their legal duties or policy functions[2];
- quasi-sovereigns and supranationals, except where this would inhibit the discharge of their organizational policy mandate;
- asset managers, sovereign wealth funds, hedge funds, pension funds, and insurance companies;
- a corporate treasury department, or Corporate Treasury Centre entering into external (non-group) transactions either on its own account or on behalf of the parent companies, subsidiaries, branches, affiliates, or joint ventures of the group it represents;

[1] The term Market Participant is generally used to refer to both firms and personnel, per the definition. However, in some cases it will be clear that a principle is by its nature more relevant to only one or the other. For example, certain principles deal primarily with business or firm-level policies and procedures rather than individual behaviors. The terms "firm" and "personnel" are occasionally used where principles focus on good practice by firms with regard to personnel in their capacity as such, and vice versa.

[2] Note that transactions by central banks for the discharge of their legal duties or policy functions may be carried out by central banks themselves or through other Market Participants, including financial institutions and supranationals that may act on an agency basis, or otherwise, on behalf of the central bank.

- family offices running treasury operations;
- benchmark execution providers;
- non-bank liquidity providers; firms running automated trading strategies, including high-frequency trading strategies, and/or offering Algorithmic Execution;
- brokers (including retail Cryptoasset brokers); investment advisers; aggregators; and analogous intermediaries/Agents;
- remittance businesses, money changers, and money services businesses in their interactions in the wholesale Cryptoasset Market;
- Cryptoasset Trading Venues;
- affirmation and settlement platforms; and
- any entity classified as an Cryptoasset Market Participant in the relevant jurisdiction(s).

As a guide, the following types of persons or organizations would not generally be considered market participants in the context of the Global Cryptoasset Standards, as they do not engage in Cryptoasset Market activities in a manner analogous to those persons or entities described in (i)-(iv) above:

- pricing display platforms;
- remittance businesses, money changers, and money services businesses in their interactions with retail customers;
- automated software protocols including, exchanges (DEXs), automated market makers (AMMs), Lenders, Yield Aggregators and other approximations of traditional financial instruments;
- private banking customers trading as individuals or via personal investment vehicles; and
- the general retail public.

The universe of Market Participants is considerably diverse in the type and level of engagement in the Cryptoasset Market. The Global Cryptoasset Standards are expected to apply to all of these Market Participants, but the details of how it may apply can depend on their underlying activities. However a different set of standards, similarly aligned, and set forth by an alternative organization with a specialized focus on alternative forms of crypto conveyance may be appropriate to address the variety and nuance pervasive in the Cryptoasset market.

In practice, the steps that different Market Participants take to align their activities with the principles of the Global Cryptoasset Standards will necessarily reflect the size and complexity of the Market Participant's Cryptoasset Market activities, and the nature of the Market Participant's engagement in the Cryptoasset Market, and will take account of Applicable Law. Ultimately, the decision of what steps should be undertaken, and in what manner, resides with each Market Participant, reflecting an appropriate internal assessment.

It is strongly recommended that all Market Participants commit to implementing the principles of these Global Cryptoasset Standards. Each Market Participant will need to apply the Global Cryptoasset Standards proportionality to its underlying business activities. Market Participants should establish appropriate processes to raise awareness within their organizations of the responsibilities personnel have with respect to the Global Cryptoasset Standards.

Annex 3 presents a "Statement of Commitment" form. The Statement, like the Code, is voluntary and Market Participants may make use of it in different ways to support the objectives of the Code, enhancing

transparency, efficiency, and functioning in the Cryptoasset Market. The Statement is accompanied by an explanatory note providing additional background.

Ethics

LEADING PRINCIPLE:

Market Participants are expected to behave in an ethical and professional manner to promote the fairness and integrity of the Cryptoasset Market.

The ethical and professional behavior of Market Participants underpins the fairness and integrity of the Cryptoasset Market. The exercise of judgement is central to acting ethically and professionally, and Market Participants (meaning both firms and their personnel) should be guided in doing so by the high-level principles below, both when applying the specific guidance in the Global Cryptoasset Standards and at all times when participating in the Cryptoasset Market.

PRINCIPLE 1

Market Participants should strive for the highest ethical standards.

Market Participants should:

- act honestly and transparently in dealings with Clients and other Market Participants;
- act fairly, dealing with Clients and other Market Participants in a consistent and appropriately transparent manner; and
- act with integrity, particularly in avoiding and confronting questionable practices and behaviors.

Market participants should not knowingly misrepresent information about the firm's regulatory and licensing status, financing services including but not limited to lending practices, data privacy, research, and marketing materials; and take all reasonable steps to ensure that Client communications contain adequate content and disclosures.

Maintaining high standards of behavior is the responsibility of:

- firms, which should promote ethical values and behavior within the organization, support efforts to promote high ethical standards in the wider Cryptoasset Market, and encourage involvement by personnel in such efforts;
- senior and front-line management, which should be pro-active in embedding and supporting the practice of ethical values within the firm's culture and be prepared to give appropriate advice to personnel; and
- personnel, who should apply judgement when facing ethical questions, expect to be held responsible for unethical behavior, and seek advice where appropriate. Personnel should report and/or escalate issues of concern to appropriate parties internally or externally, having regard to the circumstances.

PRINCIPLE 2

Market Participants should strive for the highest professional standards.

All Market Participants share a common interest in maintaining the highest degree of professionalism and the highest standards of business conduct in the Cryptoasset Market.

High standards of conduct are underpinned by:

- having sufficient knowledge of, and complying with Applicable Law;
- having sufficient relevant experience, technical knowledge, and qualifications;
- acting with competence and skill;
- applying professional judgement in following the firm's guidelines and operating procedures, including, but not limited to, methods of execution, record keeping, and ethical behavior; and
- engaging in efforts to strive for the highest standards of professionalism in the wider Cryptoasset Market.

Market Participants should have personnel who are appropriately trained and who have the necessary experience to discharge their employment duties in a professional manner. Market Participants should perform appropriate staff background screening and due diligence to hire competent and professional people and advisors that act with honesty and integrity. Ethical and professional standards should also be assessed on an ongoing basis.

Market Participants that are a Trading Venue or other intermediary should engage in good governance. This indicates such organizations should put in place a clear legal and organizational structure, clear and transparent listing and/or asset support requirements, proper liquidity, credit, financial crime, compliance and operational risk management practices and clear processes in relation to settlement and safekeeping.

PRINCIPLE 3

Market Participants should identify and address conflicts of interest.

Market Participants should identify actual and potential conflicts of interest that may compromise or be perceived to compromise the ethical or professional judgement of Market Participants. Market Participants should eliminate these conflicts or, if this is not reasonably possible, effectively manage them so as to promote fair treatment of their Clients and other Market Participants, up to and including abstaining from undertaking the relevant activity or action due to the conflict of interests.

Personnel should be aware of the potential for conflicts of interest to arise and comply with their firm's policies in these areas.

Contexts in which conflicts may arise include, but are not limited to:

- situations where personal or firm interests may conflict with those of a Client or other Market Participant, or where such a conflict arises for the Market Participant because the interests of one Client may conflict with those of another;
- personal relationships;
- gifts and corporate entertainment; and
- Personal Dealing.

Market Participants should put in place appropriate and effective arrangements to eliminate or manage conflicts of interest. This could include:

- segregation of duties and/or reporting lines;
- establishing information barriers (for example, physical segregation of certain departments and/or electronic segregation);
- altering the duties of personnel when such duties are likely to give rise to conflicts of interest;

- providing training to relevant personnel to enable them to identify and handle conflicts of interest;
- establishing declaration policies and/or records for identified conflicts of interest and personal relationships, as well as for gifts and corporate entertainment received;
- having adequate policies and procedures in relation to personal trading, outside business activities and the receipt or provision of gifts or entertainment; and
- implementing processes designed to identify, detect, and deter trading of Cryptoassets based on material non-public information, or practices that are designed to improperly or artificially manipulate the price of Cryptoassets.

Where it is concluded that a specific conflict of interest cannot reasonably be avoided or effectively managed (including by ceasing to undertake the relevant service or activity), Market Participants should disclose sufficient details of the conflict to enable the affected parties to decide beforehand whether or not they wish to proceed with the transaction or service.

Governance

LEADING PRINCIPLE:

Market Participants are expected to have a sound and effective governance framework to provide for clear responsibility for and comprehensive oversight of their Cryptoasset Market activity and to promote responsible engagement in the Cryptoasset Market.

Appropriate governance structures should be in place to promote and support the principles set out in this Code. Different firms' governance structures may vary in complexity and scope. The precise structure adopted should be commensurate with the size and complexity of the Market Participant's Cryptoasset Market activities, and the nature of the Market Participant's engagement in the Cryptoasset Market, taking into account Applicable Law.

PRINCIPLE 4

The body, or individual(s), that is ultimately responsible for the Market Participant's Cryptoasset business strategy and financial soundness should put in place adequate and effective structures and mechanisms to provide for appropriate oversight, supervision, and controls with regard to the Market Participant's Cryptoasset Market activity.

The body, or individual(s), that is ultimately responsible for the Market Participant's Cryptoasset business strategy and financial soundness should put in place:

- an operational structure with clearly defined and transparent lines of responsibility for the Market Participant's Cryptoasset Market activity;
- mechanisms to ensure the Market Participant has adequate financial resources;
- a transparent legal governance and ownership structure that reasonably protects Market Participant's interests;
- effective oversight of the Market Participant's Cryptoasset Market activity based on appropriate management information;
- an environment that encourages effective challenge to senior management charged with day-to-day responsibility for the Market Participant's Cryptoasset Market activity; and

- independent control functions and mechanisms to assess whether the Market Participant's Cryptoasset Market activities are conducted in a manner that reflects the Market Participant's operational risk and conduct requirements. Such functions should have sufficient stature, resources, and access to the body or individual(s) that is ultimately responsible for the Market Participant's Cryptoasset business strategy and financial soundness.

In implementing the above, consideration should be given to the types of activities that the Market Participant engages in, including if the Market Participant engages in the provision or usage of Electronic Trading Activities or Prime Broker services.

Separately, Market Participants who engage in Cryptoasset custody services should consider the following:

- implement the necessary operational and technological checks and balances to reduce risks associated with control and access to customer holdings to ensure sufficient segregation of transaction signing capabilities to prevent unauthorized activity / disclosure, fraud, and a single source of failure;
    i. The checks and balances should be part of a non-repudiable auditable workflow
- disclose to Clients to what degree their assets are protected under insurance in the event of a loss, and to what degree their assets are at risk in the event of bankruptcy and/or material loss.
- ensure consistent periodic reporting to Clients including account statements, corporate actions and specific Cryptoasset activity (forks, airdrops, etc.);
    i. When commercially reasonable and in-line with transparent policy, ensure that all airdrops are made available to the Client.
- If commingling of assets occurs within omnibus accounts, Market Participant should communicate this to the Client;
- Market Participant should not rehypothecate Clients' Cryptoassets held on their behalf unless explicitly agreed with the Client;
- design systems to enable a high degree of security against cyber threats, ensure operational integrity, reliability, with adequate and scalable capacity;
- conduct third-party technological audits, with respect to risk, compliance, and cybersecurity;
- ensure that periodic IT security training is provided to ensure all staff are aware of the common techniques used in malicious acts such as phishing;
- Establish formal risk management practices to identify and manage technology, operational and cyber risk such as asset identification, secure information handling, system acquisition / development and maintenance, access control and multifactor authentication for high risk access / activity, malware protection, mobile device management, encryption / cryptography / key management, custody, logging and monitoring, backup management, network security, vulnerability management, incident management and third-party management;
- put in place controls for any service outsourced or partnerships entered into, through thorough due diligence, including but not limited to:
    i. external audits;
    ii. ethical hacker support for developing partners platforms and/or continued risk assessment of integrated IT systems to ensure no risk of unauthorized access; and
- ensure a consistent level of service for every supported Cryptoasset, noting that each Cryptoasset may have a different protocol.

PRINCIPLE 5

Market Participants should embed a strong culture of ethical and professional conduct with regard to their Cryptoasset Market activities.

Market Participants should, among other things:

- expect senior management to be highly visible to relevant personnel of the Market Participant in articulating and modelling the desired practices, values, and conduct;
- take appropriate steps to promote and reinforce all relevant personnel's awareness and understanding of (i) the values and the ethical and conduct standards that should be adhered to in their engagement in the Cryptoasset Market; and (ii) Applicable Law that is relevant to them (see Principle 28); and
- make all relevant personnel (including senior management) aware that disciplinary or other actions may result from unacceptable behaviors and transgressions of the Market Participant's policies.

PRINCIPLE 6

Market Participants should have remuneration and promotion structures that promote market practices and behaviors that are consistent with the Market Participant's ethical and professional conduct expectations.

Market Participants' remuneration and promotion structures should encourage practices and behaviors that are consistent with the firm's ethical and professional conduct expectations; they should not incentivize personnel to engage in inappropriate behaviors or practices, or to take risks beyond the overall business risk parameters of the Market Participant.

Factors that should be taken into account include but are not limited to:

- the mix of pay components, such as fixed and variable;
- the form and timing of payment for the variable pay component;
- how such structures align the interest of relevant personnel with the interests of the
- firm over both short and long-term horizons; and
- appropriate mechanisms to discourage inappropriate practices or behaviors.

PRINCIPLE 7

Market Participants should have appropriate policies and procedures to handle and respond to potentially improper practices and behaviors effectively.

Market Participants should maintain policies and procedures, supported by effective mechanisms, to (i) provide confidential channels for personnel or external parties to raise concerns about potentially improper practices and behaviors and (ii) investigate and respond to such reports as appropriate.

Specifically, firms should be clear with relevant personnel and external parties about where and how to report concerns about potentially improper practices, security lapses and behaviors (including but not limited to cases of illegal, unethical, or questionable practices and behaviors) confidentially and without fear of reprisal or retribution.

Reports of potentially improper practices or behavior of the Market Participant should be investigated by independent parties or functions. Such parties or functions should possess sufficient skills and experience—and be given the necessary resources and access—to conduct the investigation.

Market Participants should complete the investigation and determine the appropriate outcome within a reasonable time frame, taking into account the nature and complexity of the matter in question. Escalation within the firm and reporting outside the firm may be appropriate before an investigation is concluded. The reports and results should be brought to the attention of the appropriate individuals within the Market Participant, and if appropriate, to relevant regulatory or public authorities.

Market Participants should review reports of improper practices and behavior, and/or client complaints, in order to identify any underlying themes and/or recurring issues, and take resulting action to improve the services offered. Such reviews may occur on a regular basis (e.g., quarterly) and in addition may be triggered by some particular metric (e.g., volume of complaints in 1 week). At a minimum, regular review is recommended.

PRINCIPLE 8

Market Participants that issue Cryptoassets should establish appropriate protocols and processes.

To this end, Market Participants should:

- follow appropriate due diligence protocols during a capital raising exercise and implement due diligence protocols proportionate to the size and scale of the business;
- review the process and legal requirements for Cryptoasset services (such as corporate disclosure, proxy voting, payment of dividends or other distributions, stock splits) to be provided to all security holders;
- commit to, where appropriate, treating traditional equity and digital equity equally.
- comply with the applicable legal requirements for the corporate form chosen and designate a legal representative, where required;
- take reasonable steps to safeguard investor and customer's Confidential Information that if disclosed to an unauthorized party could lead to reputational damage, regulatory fines, and financial losses, and where possible including features within the Cryptoasset design that promote data privacy;
- utilize Cryptoasset standards that align with industry and regulatory accepted best practices to increase interoperability and standardization;
- note that the issuance of Cryptoassets may bring the product and activities around the product into a regulated space; and
- assign ultimate responsibility for each protocol or process to an individual and/or function of the business (e.g., MLRO or the Board of Directors) and have regular review periods to confirm ownership.

PRINCIPLE 9

Market Participants should take into consideration applicable regulatory and/or legal requirements, commitments and protections related to secondary market activities.

To this end, Market Participants should:

- obtain the necessary regulatory status according to the law of the jurisdiction that the body, or individual(s), is operating in. This may be as:

    i. An intermediary (such as a broker), that facilitates the sale of securities by a Client – which could be on an advised basis, an agency – or Principal-basis, or as a pure arranger; or

    ii. As the operator of an organized Trading Venues, such as an alternative trading system or exchange – this would typically apply to firms that operate trading systems bringing together multiple buying and selling interests through an organized system for publicizing, matching, and executing such trades.

- consider the legal requirements for recording the transfer of title to securities in their jurisdictions. If this requires trades to be registered by a licensed central securities depository (CSD), a transaction in a Cryptoasset that is recorded using blockchain technology may also need to be registered on the books and records of a CSD. However, if this is not necessary, Market Participants should acknowledge that this may result in a lower level of legal or regulatory protection for Market Participants that rely instead on recordkeeping via the blockchain only;

- consider the impact of the insolvency of a participant in the transaction and acknowledge that certain national insolvency laws will provide rights to unwind transactions that have already been executed;

- If the system requires the creation of a new transaction to add a new "block" to the chain in order to unwind a previous transaction Market Participants carefully analyses the applicable insolvency laws in order to ensure that the legal implications of its operation can be clearly understood in scenarios where a participant is solvent and where it is insolvent;

- be aware of arrangements for ensuring settlement finality. Some jurisdictions have laws designed to ensure settlement finality by protecting orders processed through a settlement system, even if a participant has become insolvent after (or shortly prior to) the entry of the order into the system. If an arrangement for the trading and settlement of Cryptoasset is not subject to these laws, then participants may not have equivalent legal protection to that available for traditional securities; and

- have a clear understanding of whether Cryptoasset Market Participants are able to benefit from the legal protections available to other financial market infrastructures (FMIs); and in any event, Cryptoasset Market Participants will have a clear understanding of what the legal and practical implications of a disruptive event (such as a participant's insolvency) on the operation of system and the settlement of the trades processed through it.

If operating as a regulated intermediary, such Market Participants should:

- establish appropriate terms of business with their Clients and counterparties;

- provide to Clients appropriate information regarding the nature of the Cryptoasset and/or ensure that the trade is suitable or otherwise appropriate for the Client;

- avoid and/or manage conflicts between the interests of Clients and those of ourselves and other Clients;
- provide appropriate information regarding the costs of execution of the transactions; and
- subject to the basis on which legal title to the Cryptoasset is held / recorded, establish suitable custody arrangements in respect of the Cryptoassets purchased or held for Clients. Where the Cryptoasset is recorded on a blockchain-based ledger, Market Participants should understand clearly: how Applicable Law treats the establishment of title to the security represented by the Cryptoasset; whether typical custody structures for securities in a jurisdiction can be applied to a Cryptoasset; and the implications for the Client of the insolvency of the organization or its custodian.

If operating as a regulated Trading Venue, such Market Participants should:

- establish a set of rules to govern the activities of Market Participants using the platform;
- require participants to meet specific conditions in order to have access to the market;
- monitor trading activity in order to identify breaches, disorderly trading, or market abuse;
- publish trades to the market, which may involve assessing the level of liquidity in a particular security in order to determine whether or not a trade must be published;
- report trades executed on the system to the regulatory authority;
- ensure that the trading system is resilient, has adequate capacity to handle the volume of trades expected, and ensures business continuity in the event of severe disruption; and
- ensure the orderly functioning of the market so that it does not pose a risk to participants or the financial system as a whole; and
- apply appropriate AML ("anti-money-laundering") / KYC ("know-your-customer") / CDD ("customer-due-diligence") considerations for Users / Participants, plus timely reporting to Authorities (e.g., SARs ("suspicious-activity-reports")).

Execution

LEADING PRINCIPLE:

Market Participants are expected to exercise care when negotiating and executing transactions in order to promote a robust, fair, open, liquid, and appropriately transparent Cryptoasset Market.

The Cryptoasset execution landscape is diverse, with execution taking place through many different channels and with Market Participants taking on different roles with regard to that execution. All Cryptoasset Market Participants, regardless of their role in the execution of transactions, should behave with integrity to support the effective functioning of the Cryptoasset Market.

PRINCIPLE 10

Market Participants should be clear about the capacities in which they act.

Market Participants should understand and clearly communicate their roles and capacities in managing orders or executing transactions. Market Participants may have a standing agreement or other terms of business as to their roles that govern all trades, or they may manage their relationship by determining their roles on a trade-by-trade basis. If a Market Participant wishes to vary the capacity in which it or its counterpart acts, any such alternative arrangement should be agreed by both parties.

A Market Participant receiving a Client order may:

- act as an Agent, executing orders on behalf of the Client pursuant to the Client mandate, and without taking on market risk in connection with the order; or
- act as a Principal taking on one or more risks in connection with an order, including credit risk and varying degrees of market risk. Principals act on their own behalf and there is no obligation to execute the order until both parties are in agreement. Where the acceptance of an order grants the Principal executing the order some discretion, it should exercise this discretion reasonably, fairly, and in such a way that is not designed or intended to disadvantage the Client.

PRINCIPLE 11

Market Participants should handle orders fairly and with transparency in line with the capacities in which they act.

Market Participants are expected to handle orders with fairness and transparency. How this is done, and what the relevant good practices are, vary depending upon the role in which those Market Participants are acting, as described in Principle 10 above. This principle takes into account both Principal and Agency models as well as Trading Venues and OTC desks.

ROLES

Irrespective of their role, Market Participants handling orders should:

- have clear standards in place that strive for a fair and transparent outcome for the Client;
- be truthful in their statements;
- use clear and unambiguous language;
- make clear whether the prices they are providing are firm or merely indicative;
- have adequate processes in place to support the rejection of Client orders for products they believe to be inappropriate for the Client;
- not enter into transactions with the intention of disrupting the market (see Principle 14 in Execution for further guidance); and
- provide all relevant disclosures and information to a Client before negotiating a Client order, thereby allowing the Client to make an informed decision as to whether to transact or not.

Market Participants should make Clients aware of such factors as:

- how orders are handled and transacted, including whether orders are aggregated or time prioritized;
- the potential for orders to be executed either electronically or manually, depending on the disclosed transaction terms;
- the various factors that may affect the execution policy, which would typically include positioning, whether the Market Participant managing Client orders is itself taking on the associated risk or

not, prevailing liquidity and market conditions, other Client orders, and/or a trading strategy that may affect the execution policy;
- where discretion may exist or may be expected, and how it may be exercised;
- the basis on which trade requests and/or orders might be rejected; and
- whenever possible, what the time-stamping policy is and whether it is applied both when the order is accepted and when it is triggered or executed (see Principle 45 in Risk Management and Compliance for further guidance).

Principal

Market Participants handling Client orders in a Principal role should:

- disclose the terms and conditions under which the Principal will interact with the Client, which might include:
  - ✓ that the Principal acts on its own behalf as a counterparty to the Client;
  - ✓ how the Principal will communicate and transact in relation to requests for quotes, requests for indicative prices, discussion or placement of orders, and all other expressions of interest that may lead to the execution of transactions; and
  - ✓ how potential or actual conflicts of interest in Principal-dealing and market- making activity may be identified and addressed;
- establish clarity regarding the point at which market risk may transfer;
- have market-making and risk management activity, such as hedging, commensurate with their trading strategy, positioning, risk assumed, and prevailing liquidity and market conditions; and
- have internal Mark Up policies consistent with applicable guidelines elsewhere in this Global Cryptoasset Standards.

Agent

Market Participants handling Client orders in an Agent role should:

- communicate with the Client regarding the nature of their relationship;
- seek to obtain the result requested by the Client;
- establish a transparent order execution policy that should supply information relevant to the Client order that may include:
  - ✓ information on where the firm may execute the Client orders;
  - ✓ the factors affecting the choice of execution venues; and
  - ✓ information as to how the Agent intends to provide for the prompt, fair, and expeditious execution of the Client order;
- be transparent with the Client about their terms and conditions, which clearly set out fees and commissions applicable throughout the time of the agreement; and
- share information relating to orders accepted on an Agency basis with any market-making or Principal trading desks only as required to request a competitive quote. (See Principle 21 in Information Sharing for further guidance.)

Market Participants acting as OTC desks should meet similar expectations as described above for Market Participants handling Client orders in an Agent role. OTC desks may operate via voice, such as Voice Brokers, or may operate either partially or wholly electronically.

Cryptoasset Trading Venues

Market Participants operating Cryptoasset Trading Venues should:

- have rules that are transparent to users, written in plain language and publicly available, in accordance with the principles set forth in this document;
- make clear any restrictions or other requirements that may apply to the use of the electronic quotations;
- establish clarity regarding the point at which market risk may transfer;
- have appropriate disclosure about subscription services being offered and any associated benefits, including market data (so that Clients have the opportunity to select among services);
- explicitly state – when hosting multiple liquidity providers – market data policies within applicable disclosure documents (including rulebooks, guidelines, etc.), including at a minimum: what level of detail is available, which user types they are available to, and with what frequency and latency this market data is available;
- incorporate appropriate market surveillance techniques:
  - ✓ monitor trading activity and establish a benchmark of what represents normal and abnormal market activity.
  - ✓ employ systems to identify disruptions and market abuse which could result in disorderly market conditions.
  - ✓ identify and escalate breaches of normal market activity in a timely manner.
  - ✓ have processes in place to communicate potential market abuse, abnormal activity, and financial crime to the appropriate organizations, as well as co-operate with them fully until resolved in the eyes of the relevant organization.
- conduct Cryptoasset due diligence:
  - ✓ set and disclose the requirements, thresholds, due diligence, and approval processes that apply before making Cryptoassets accessible on the venue for trading (often referred to as "listing").
  - ✓ disclose how Cryptoassets accessible for trading are assessed to determine they fall outside the remit of financial laws (i.e., Howey test).
  - ✓ disclose exclusion categories (i.e., the types of Cryptoassets will not be added to the trading venue), if any.
  - ✓ disclose policies and procedures around the levels of compensation, if any, which are accepted for adding Cryptoassets to the Trading Venue.
  - ✓ disclose conditions for tokens to remain accessible for trading on the platform, such as liquidity thresholds and periodic disclosure requirements, as well as the circumstances in which trading may be suspended

New Cryptoasset Issuances

For new Cryptoasset issuances, provide the following additional relevant disclosures and information to the Client:

- The name of the token, its function and purpose, and its technical specifications;
- Cautionary language to token purchasers regarding the financial risks associated with purchasing Cryptoassets;

- Cautionary language that token purchasers should not purchase Cryptoassets that they cannot afford to lose;
- Cautionary language that the project may never be executed, in which case the Cryptoassets have no use or value;
- Details as to the token issuance process, publicized through secure mediums, protecting Cryptoasset purchasers and reducing the risk of fraud;
- Unless precluded under non-disclosure agreements, involvement with previous Cryptoasset issuances, including failure or success of the project;
- The usage, platform service and other rights that Cryptoasset purchasers have and don't have, including restrictions on transferability;
- A description of rights token purchasers have and don't have in case the Cryptoasset issuer winds down its operations;
- The anticipated length of the token distribution period, funding caps that are proportionate to the expected project and technology development costs and timelines and any refund mechanisms;
- The rules that govern total token supply or inventory of tokens, including, and how in the future new tokens can be created or how issued tokens can be destroyed;
- The factors that may impact the number of tokens in circulation such as lock-up periods and transfer restrictions, including the timeline or mechanisms under which such lock-ups and transfer restrictions will end;
- The governance for token inventory that is retained by the project or related entities;
- If the tokens are issued through smart contract, a detailed description thereof and the latest smart contract address;
- Where applicable, details of the token vault or the token lock smart contract address;
- Commitment that the proceeds from the token sales will only be used for the purposes set forth in the whitepaper, and in accordance with the budget provided; and
- Confirmation that the tokens and smart contracts have been subjected to a third-party security audit proportionate to the nature, scale, and complexity of the project

Issuing or Listing Cryptoassets

Additionally, Market Participants issuing or listing Cryptoassets should:

- put in place governance arrangements that are clear and transparent, promote the safety and efficiency of the platform, conform to applicable market conduct standards and expectations, facilitate trusted price formation of Cryptoassets and support the stability of the broader Cryptoasset system and the objectives of relevant stakeholders;
- disclose the name, address, and company registration number of the Market Participant legal entity, as well as the name, contact details and experience of Market Participants' officers, directors and senior management;
- disclose Market Participant's licensing status, if any, as well as the regulations that such licensing status subjects the Market Participant;
- disclose any material cross-holdings or material conflicts of interest between the Market Participant, Cryptoasset issuers, Cryptoasset service providers, Trading Venues, intermediaries, or funds;
- put in place and publish fair and non-discriminatory standards for the admission of new Cryptoassets on a Trading Venue;

- provide a proper balance of opportunities and risks, including things that must happen for the project to be successful, and how the management team plans to address and mitigate these risks and dependencies;
- Give the rationale for using blockchain, the consensus mechanism, the stage of development (test-net or main-net), the current numbers of users and nodes that are running or are reasonably expected to run in the future, whether nodes can be run by anyone in a decentralized fashion or on a permissioned basis and the applicable block explorer;
- Obtain appropriate regulatory permissions for our trading venue activities in the jurisdiction in which we operate;
- Comply with the legal and regulatory requirements of the primary issuer for all instruments listed or traded on our venue;
- Ensure all systems and controls are effective and appropriate for the size and scale of the business;
- Carry out KYC and AML checks to establish the identity of the beneficial owner; and
- Undertake periodic refreshes of identity and additional documentation for certain accounts as required if they are frequently trading or engaged in large volumes of activity.

Market Participants operating anonymous Trading Venues that feature unique identifiers ("tags") should, where applicable:

- have appropriate disclosure to all users of what specific counterparty information is provided for tags, and to whom this information is provided;
- have appropriate disclosure to all users indicating at what point in a transaction a user tag is provided to their counterparty;
- have disclosure documents (including rulebooks, guidelines, etc.) that contain clear policies related to how tags are assigned and managed, including policies related to re-tagging; and
- maintain audit trails for all tag assignments and re-tag.

Market Participants acting as Clients should:

- be aware of the responsibilities they should expect of others as highlighted above;
- be aware of the risks associated with the transactions they request and undertake;
- regularly evaluate the execution they receive.
  - ✓ pricing transactions in a manner that is transparent and is consistent with the risk borne in accepting such transactions; and
  - ✓ establishing and enforcing internal guidelines and procedures for collecting and executing Fixing Orders.

Market Participants should actively seek to obtain legal entity identifiers (LEI) for their entities that are providing services in Cryptoasset markets. Obtaining LEI will allow trading credibility and provide protection when Market Participants decide to trade with another party. LEI can secure identity, provide transparency of the legitimacy of a company, facilitate the reporting of transactions, and assist in adhering to legal and regulatory requirements. LEI can help to create a healthy and well-functioning Cryptoasset ecosystem across borders.

Indicative Examples of Acceptable Practices:

- ✓ transacting an order over time before, during, or after its fixing calculation window, so long as not to intentionally negatively impact the market price and outcome to the Client.

PRINCIPLE 12

Market Participants should handle orders fairly, with transparency, and in a manner consistent with the specific considerations relevant to different order types.

Market Participants should be aware that different order types may have specific considerations for execution.

Market Participants handling a Client's Stop Loss Order should:

- obtain from the Client the information required to fully define the terms of a Stop Loss Order, such as the reference price, order amount, time period, and trigger;
- disclose to Clients whether risk management transactions may be executed close to a Stop Loss Order trigger level, and that those transactions may impact the reference price and result in the Stop Loss Order being triggered.

Indicative Examples of Unacceptable Practices:

- ✓ trading or otherwise acting in a manner designed to move the market to the Stop Loss level; and
- ✓ offering Stop Loss Orders on a purposefully loss-making basis.

Market Participants filling a Client order, which may involve a partial fill, should:

- be fair and reasonable based upon prevailing market circumstances, and any other applicable factors disclosed to the Client, in determining if and how a Client order is filled, paying attention to any other relevant policies;
- make a decision on whether, and how, to fill a Client order, including partial fills, and communicate that decision to the Client as soon as practicable; and fully fill Client orders they are capable of filling within the parameters specified by the Client, subject to factors such as the need to prioritize among Client orders and the availability of the Market Participant's credit line for the Client at the time.

Market Participants handling a Client's order to transact at a particular fixing rate (Fixing Order):

- should understand the associated risks and be aware of the appropriate procedures;
- should not, whether by collusion or otherwise, inappropriately share information or attempt to influence the exchange rate;
- should not intentionally influence the benchmark fixing rate to benefit from the fixing, whether directly or in respect of any Client-related flows at the underlying fixing.

Indicative Examples of Unacceptable Practices:

- buying or selling a larger amount than the Client's interest within seconds of the fixing calculation window with the intent of inflating or deflating the price against the Client;
- buying or selling an amount shortly before a fixing calculation window such that there is an intentionally negative impact on the market price and outcome to the Client;

- showing large interest in the market during the fixing calculation window with the intent of manipulating the fixing price against the Client;
- informing others of a specific Client dealing at a fixing rate; and
- acting with other Market Participants to inflate or deflate a fixing rate against the interests of a Client. (See Principles 21 and 22 in Information Sharing for further guidance.)

Finally, Market Participants handling orders that have the potential to have sizable market impact should do so with particular care and attention. For example, there are certain transactions that may be required in the course of business, such as those related to merger and acquisition activity, which could have a sizable impact on the market.

PRINCIPLE 13

A Market Participant should only Pre-Hedge Client orders when acting as a Principal, and should do so fairly and with transparency.

Pre-Hedging is the management of the risk associated with one or more anticipated Client orders, designed to benefit the Client in connection with such orders and any resulting transactions.

Market Participants may Pre-Hedge for such purposes and in a manner that is not meant to disadvantage the Client or disrupt the market. Market Participants should communicate their Pre-Hedging practices to their Clients in a manner meant to enable Clients to understand their choices as to execution.

- In assessing whether Pre-Hedging is being undertaken in accordance with the principles above, a Market Participant should consider prevailing market conditions (such as liquidity) and the size and nature of the anticipated transaction.
- While undertaking Pre-Hedging, a Market Participant may continue to conduct ongoing business, including risk management, market making, and execution of other Client orders. When considering whether Pre-Hedging is being undertaken in accordance with the principles above, Pre-Hedging of a single transaction should be considered within a portfolio of trading activity, which takes into account the overall exposure of the Market Participant.
- When a Market Participant is acting as an Agent, the Market Participant should not Pre-Hedge.

See Annex 1 for a set of stylized examples regarding Pre-Hedging.

PRINCIPLE 14

Market Participants should not request transactions, create orders, or provide prices with the intent of disrupting market functioning or hindering the price discovery process.

Market Participants should not engage in trading strategies or quote prices with the intent of hindering market functioning or compromising market integrity. Such strategies include those that may cause undue latency, artificial price movements, or delays in other Market Participants' transactions and result in a false impression of market price, depth, or liquidity. Such strategies also include collusive and/or manipulative practices, including but not limited to those in which a trader enters a bid or offer with the intent to cancel before execution (sometimes referred to as "spoofing," "flashing." or "layering") and other practices that create a false sense of market price, depth, or liquidity (sometimes referred to as "quote stuffing" or "wash trades").

Market Participants providing quotations should always do so with a clear intent to trade. Prices provided for reference purposes only should clearly be labelled as such.

Market Participants should give appropriate consideration to market conditions and the potential impact of their transactions and orders. Transactions should be conducted at prices or rates based on the prevailing market conditions at the time of the transaction. Exceptions to this, such as historical rate rollovers, should be covered by internal compliance policies.

Without limitation, Market Participants handling Client orders may decline a transaction when there are grounds to believe that the intent is to disrupt or distort market functioning. Market Participants should escalate as appropriate.

See Annex 1 for a set of stylized examples regarding handling of orders and market disruptions.

PRINCIPLE 15

Market Participants should understand how reference prices, including highs and lows, are established in connection with their transactions and/or orders.

This understanding should be supported by appropriate communications between the parties, which may include disclosures. In the event that a third-party pricing source is an input in establishing this reference price, both parties should understand how that pricing measure is determined and what the contingency arrangements are in the event that the third-party pricing is unavailable.

PRINCIPLE 16

The Mark Up applied to Client transactions by Market Participants acting as Principal should be fair and reasonable.

Mark Up is the spread or charge that may be included in the final price of a transaction in order to compensate the Market Participant for a number of considerations, which might include risks taken, costs incurred, and services rendered to a particular Client.

Market Participants should promote transparency by documenting and publishing a set of disclosures regarding their Cryptoasset business that, among other things:

- Makes it clear to Clients that their final transaction price may be inclusive of Mark Up;
- Makes it clear to Clients that different Clients may receive different prices for transactions that are the same or similar;
- Helps Clients understand the determination of Mark Up, such as by indicating the factors that may contribute to the Mark Up (including those related to the nature of the specific transaction and those associated with the broader Client relationship, as well as any relevant operating costs); and
- Discloses to Clients how Mark Up may impact the pricing and/or execution of any order linked to or triggered at a specific level.

Firms should have policies and procedures that enable personnel to determine an appropriate and fair Mark Up. These policies and procedures should include, at a minimum:

- guidance that prices charged to Clients should be fair and reasonable considering applicable market conditions and internal risk management practices and policies; and

- guidance that personnel should always act honestly, fairly, and professionally when determining Mark Up, including not misrepresenting any aspect of the Mark Up to the Client.

Market Participants should have processes to monitor whether their Mark Up practices are consistent with their policies and procedures, and with their disclosures to Clients. Mark Up should be subject to oversight and escalation within the Market Participant.

See Annex 1 for a set of stylized examples regarding Mark Up.

PRINCIPLE 17

Market Participants should identify and resolve trade discrepancies as soon as practicable to contribute to a well-functioning Cryptoasset Market.

Market Participants should have effective policies and procedures designed to minimize the number of trade discrepancies arising from their Cryptoasset Market activities and should manage such discrepancies promptly.

Market Participants acting as Prime Brokers play a unique role in assuming the credit risk of authorized trades executed by their Prime Brokerage Clients. Where the Client identity is known, Prime Brokerage Clients and executing dealers are responsible for re- solving trade discrepancies to achieve timely amendments and matching of trade terms through the Prime Broker.

When anonymous market access is provided, the access provider should assist in the resolution of trade discrepancies.

See Principle 58 for Confirmation and Settlement discrepancies.

PRINCIPLE 18

Market Participants acting as Voice Brokers should only employ name switching where there is insufficient credit between parties to the transaction.

Voice Brokers that undertake name switching should:

- have proper controls and appropriately monitor such transactions;
- have proper approvals;
- execute, and book, such transactions as promptly as possible, consistent with the appropriate protection of related Confidential Information; and
- maintain proper records of such activity.

A dealer should not solicit or accept favors from a Voice Broker for switching names.

PRINCIPLE 19

Market Participants employing last look should be transparent regarding its use and provide appropriate disclosures to Clients.

Last look is a practice utilized in Electronic Trading Activities whereby a Market Participant receiving a trade request has a final opportunity to accept or reject the request against its quoted price. Market Participants receiving trade requests that utilize the last look window should have in place governance and controls around its design and use, consistent with disclosed terms. This may include appropriate management and compliance oversight.

A Market Participant should be transparent regarding its last look practices in order for the Client to understand and to be able to make an informed decision as to the manner in which last look is applied to their trading. The Market Participant should disclose, at a minimum, explanations regarding whether, and if so how, changes to price in either direction may impact the decision to accept or reject the trade, the expected or typical period of time for making that decision, and more broadly the purpose for using last look.

If utilized, last look should be a risk control mechanism used in order to verify validity and/or price. The validity check should be intended to confirm that the transaction details contained in the request to trade are appropriate from an operational perspective and there is sufficient available credit to enter into the transaction contemplated by the trade request. The price check should be intended to confirm whether the price at which the trade request was made remains consistent with the current price that would be available to the Client.

In the context of last look, the Market Participant has sole discretion, based upon the validity and price check processes, over whether the Client's trade request is accepted or not, leaving the Client with potential market risk in the event the trade request is not accepted. Accordingly, and consistent with related principles in the Global Cryptoasset Standards:

- Last look should not be used for purposes of information gathering with no intention to accept the Client's request to trade.
- Confidential Information arises at the point the Market Participant receives a trade request at the start of the last look window, and use of such Confidential Information should be consistent with Principles 21 and 22 on Information Sharing.
- Market Participants should not conduct trading activity that utilizes the information from the Client's trade request during the last look window. Such trading activity would include (1) any pricing activity on Cryptoasset Trading Venue that incorporates information from the trade request and (2) any hedging activity that incorporates information from the trade request. Such activity would risk signaling to other Market Participants the Client's trading intent and could move market prices against the Client. In the event that the Client's trade requests were subsequently rejected, such trading activity could disadvantage the Client.

This guidance does not apply to an arrangement that features all of the following characteristics:

1. An explicit understanding that the Market Participant will fill the Client's trade request without taking on market risk in connection with the trade request by first entering into offsetting transactions in the market; and
2. The volume traded in the last look window will be passed on to the Client in its entirety; and
3. This understanding is appropriately documented and disclosed to the Client.

It is good practice for Market Participants to be available to engage in a dialogue with Clients regarding how their trade requests have been handled, including the appropriate treatment of information associated with those trade requests. Such dialogue could include metrics that facilitate transparency around the pricing and execution of the Client's trade requests and assist a Client in evaluating the handling of its trade requests in order to evaluate whether the execution methodology continues to meet its needs over time.

PRINCIPLE 20

Market Participants providing algorithmic trading or aggregation services to Clients should provide adequate disclosure regarding how they operate.

Market Participants may provide Clients with algorithmic trading services that use computer programs applying algorithms to determine various aspects, including price and quantity of orders.

Market Participants may also provide aggregation services to Clients, services that pro- vide access to multiple liquidity sources or execution venues and that may include order routing to those liquidity sources or venues.

Market Participants providing algorithmic trading or aggregation services to Clients should disclose the following:

- a clear description of the Algorithmic Execution strategy or the aggregation strategy and sufficient information to enable the Client to evaluate the performance of the service, in a manner that is consistent with appropriate protection of related Confidential Information;
- whether the algorithm provider or the aggregation service provider could execute as Principal;
- the fees applicable to the provision of the services;
- in the case of algorithmic trading services, general information regarding how routing preferences may be determined; and
- in the case of aggregation services, information on the liquidity sources to which access may be provided.

Market Participants providing algorithmic trading or aggregation services should disclose any conflicts of interest that could impact the handling of any Client order (for example, arising from their interaction with their own Principal liquidity, or particular commercial interests in trading venues or other relevant service providers) and how such conflicts are addressed.

Clients of algorithmic trading providers should use such data and disclosed information in order to evaluate, on an ongoing basis, the appropriateness of the trading strategy to their execution strategy.

Clients that use an aggregator to access trading venues should understand the parameters that will define the prices displayed by the aggregator.

Market Participants providing algorithmic trading or aggregation services should provide services that perform in the manner disclosed to the Client.

Information Sharing

LEADING PRINCIPLE:

Market Participants are expected to be clear and accurate in their communications and to protect Confidential Information to promote effective communication that supports a robust, fair, open, liquid, and appropriately transparent Cryptoasset Market.

I. Handling Confidential Information

PRINCIPLE 21

Market Participants should clearly and effectively identify and appropriately limit access to Confidential Information.

Confidential Information includes the following information not in the public domain received or created by a Market Participant:

1) Cryptoasset Trading Information. This can take various forms, including information relating to the past, present, and future trading activity or positions of the Market Participant itself or of its Clients, as well as related information that is sensitive and is received or produced in the course of such activity. Examples include but are not limited to:
   - ✓ details of a Market Participant's order book;
   - ✓ other Market Participants' Axes;
   - ✓ spread matrices provided by Market Participants to their Clients; and
   - ✓ orders for benchmark fixes.
2) Designated Confidential Information. Market Participants may agree to a higher standard of non-disclosure with respect to confidential, proprietary, and other information, which may be formalized in a written non-disclosure or a similar confidentiality agreement.

Identification of Confidential Information should be in line with any legal or contractual restrictions to which the Market Participant may be subject.

Market Participants should limit access to and protect Confidential Information.

- Market Participants should not disclose Confidential Information except to those internal or external parties who have a valid reason for receiving such information, such as to meet risk management, legal, and compliance needs.
- Market Participants should not disclose Confidential Information to any internal or external parties under any circumstances where it appears likely that such party will misuse the information.
- Confidential Information obtained from a Client, prospective Client, or other third party is to be used only for the specific purpose for which it was given, except as provided above or otherwise agreed with a Client.
- Market Participants should disclose at a high level how Confidential Information, in the form of Cryptoasset Trading Information, is shared and handled internally in accordance with this Principle.
- Market Participants acting as Prime Brokers should have an appropriate level of separation between their prime brokerage business and their other sales and trading business.
  - ✓ To avoid any potential conflict of interest, a Prime Broker should have appropriate information barriers in place.
  - ✓ Prime Brokers should be transparent as to the standards they require and adopt.

Operators of Trading Venues that feature tags should ensure that the practice of "retagging" is fit for purpose, and not used to facilitate trading among participants where one party has already previously requested to avoid facing another.

For a discussion of Market Color, please see Principle 24.

PRINCIPLE 22

Market Participants should not disclose Confidential Information to external parties, except under specific circumstances.

Market Participants should disclose Confidential Information only under certain circumstances. These may include, but are not limited to, disclosure:

- to Agents, market intermediaries (such as brokers or Trading Venues), or other Market Participants to the extent necessary for executing, processing, clearing, novating, or settling a transaction;
- with the consent of the counterparty or Client;
- required to be publicly disclosed under Applicable Law, or as otherwise requested by a relevant regulatory or public authority;
- as requested by a central bank acting for policy purposes; and
- to advisors or consultants on the condition that they protect the Confidential Information in the same manner as the Market Participant that is disclosing the Confidential Information to such advisors or consultants.

Market Participants should make best efforts to avoid disclosing Client ownership of a specific public wallet address to unapproved parties.

Market Participants may actively choose to share their own prior positions and/or trading activity so long as that information does not reveal any other party's Confidential Information and the information is not shared in order to disrupt market function or hinder the price discovery process, or in furtherance of other manipulative or collusive practices.

Market Participants should only ask for Confidential Information where it is appropriate to do so consistent with Principle 21.

When determining whether to release Confidential Information, Market Participants should take into account Applicable Law, as well as any agreed-to restrictions that may limit the release.

II. Communications

PRINCIPLE 23

Market Participants should communicate in a manner that is clear, accurate, professional, and not misleading.

Communications should be easily understood by their intended recipient. Therefore, Market Participants should use terminology and language that is appropriate for the audience and should avoid using ambiguous terms. To support the accuracy and integrity of information, Market Participants should:

- attribute information derived from a third party to that third party (for example, a
- news service);
- identify opinions clearly as opinions;
- not communicate false information;

- exercise judgement when discussing rumors that may be driving price movements, identify rumors as rumors, and not spread or start rumors with the intention of moving markets or deceiving other Market Participants;
- not provide misleading information in order to protect Confidential Information—for example, when executing partial orders. Accordingly, Market Participants could, if asked, decline to disclose whether their request to transact is for the full amount rather than inaccurately suggest that it is for the full amount; and
- notify Clients of their intention to support forked assets as soon as commercially reasonable.

Market Participants should be mindful that communications by personnel reflect on the firm they represent as well as the industry more broadly.

PRINCIPLE 24

Market Participants should communicate Market Color appropriately and without compromising Confidential Information.

The timely dissemination of Market Color between Market Participants can contribute to an efficient, open, and transparent Cryptoasset Market through the exchange of information on the general state of the market, views, and anonymized and aggregated flow information.

Firms should give clear guidance to personnel on how to appropriately share Market Color. In particular, communications should be restricted to information that is effectively aggregated and anonymized.

To this end:

- communications should not include specific Client names, other mechanisms for communicating a Client's identity or trading patterns externally (for example, code names that implicitly link activity to a specific Market Participant), or information specific to any individual Client;
- Client groups, locations, and strategies should be referred to at a level of generality that does not allow Market Participants to derive the underlying Confidential Information;
- communications should be restricted to sharing market views and levels of conviction, and should not disclose information about individual trading positions;
- flows should be disclosed only by price range and not by exact rates relating to a single Client or flow, and volumes should be referred to in general terms, other than publicly reported trading activity;
- option interest not publicly reported should only be discussed in terms of broadly observed structures and thematic interest;
- references to the time of execution should be general, except where this trading information is broadly observable;
- Market Participants should take care when providing information to Clients about the status of orders (including aggregated and anonymized Fixing Orders) to protect the interests of other Market Participants to whom the information relates (this is particularly true when there are multiple orders at the same level or in close proximity to one another);
- Market Participants should not solicit Confidential Information in the course of providing or receiving Market Color;
- operators of Trading Venues that feature tags should only disclose user information (color) that has been clearly stated in their disclosure documents (including rulebooks, guidelines, etc.); and

- if feasible, anonymous Trading Venues should strive to make available to users whether a counterparty or potential counterparty to a trade has represented that it has signed a Statement of Commitment to the current version of the Global Cryptoasset Standards.[3]

See Annex 1 for a set of stylized examples of Market Color communications.

PRINCIPLE 25

Market Participants should provide personnel with clear guidance on approved modes and channels of communication.

Market Participants should communicate with other Market Participants through approved methods of communication that allow for traceability, auditing, record keeping, and confidentiality. Standards of information security should apply regardless of the specific mode of communication in use. Where possible, Market Participants should maintain a list of approved modes of communication and it is recommended that communication channels on sales and trading desks be recorded, particularly when being used to transact or share Market Color. Market Participants should give consideration, under exceptional circumstances (for example, in an emergency and for business continuity purposes), to allowing the use of unrecorded lines but should provide guidance to personnel regarding any permitted use of such unrecorded lines or devices.

PRINCIPLE 26

Market Participants are encouraged to adopt appropriate policies and procedures when providing investor disclosure.

To this end, Market Participants should take consideration of the following:

- ensure a reasonable level of disclosure in order to minimize information asymmetry between issuers, promoters, and investors.
    i. continue communicating with investors following a Cryptoasset offering and will post regular updates on progress;
    ii. avoid selective disclosure at all times and provide fair access and accurate information to all investors in a timely manner; and
    iii. make obvious to investors potential risks.
- Where Market Participants are issuing Cryptoassets that are analogous to existing financial instruments, they should produce the required documents, such as a prospectus for the issuance of Cryptoassets that are analogous to certain investment contracts.
- Where a prospectus, investment memorandum or similar offering document is needed, ensure that it complies with all Applicable Law and contains the necessary material to an investor being adequately informed to make an assessment of:
    i. the financial condition of the issuer and of any guarantor;
    ii. the rights attaching to the securities and;

[3] The responsibility of conveying accurate and up-to-date Statement of Commitment signatory status to the Trading Venues falls entirely on the user, whereas the Trading Venues is responsible only for storing and reporting this information as presented by that user and is not making any representation regarding the conduct of the user. Should there be any changes to the Statement of Commitment status of the user, the obligation is on the user to update the Trading Venues with that information.

iii. the reasons for the issuance and its impact on the issuer, including:
   1. detailed information on the issuer's venture;
   2. the features and rights attached to the securities being issued;
   3. the terms and conditions and expected timetable of the offer;
   4. the use of the proceeds of the offer; and
   5. the specific risks related to the underlying technology and any related contingency plans.

- ensure that all disclosure documents and information is written and presented in an easily analyzable and comprehensible form.
  i. communicate financial promotions for products and services, whether regulated or unregulated, in a way which is clear, fair, and not misleading.
  ii. do not overstate the potential return from the Cryptoasset.
- In respect of financial promotions, acknowledge that financial promotions such as communications to potential investors about the Cryptoasset or the offering may be a regulated activity in one or more jurisdictions.
  i. ensure to take advice on financial promotion rules in all applicable jurisdictions.
  ii. ensure that relevant potential investor communications are approved by an authorized person.

Risk Management and Compliance

LEADING PRINCIPLE:

Market Participants are expected to promote and maintain a robust control and compliance environment to effectively identify, manage, and report on the risks associated with their engagement in the Cryptoasset market.

I. Frameworks for Risk Management, Compliance, and Review

Appropriate risk management, compliance, and review structures should be in place to manage and mitigate the risks that arise from a Market Participant's activities in the Cryptoasset market. These structures vary in complexity and scope, but generally share some common aspects. For example:

The responsibility rests with the business unit which owns the risk it incurs in conducting its activities.

In addition, there may be both a risk management function that oversees risk-taking activities and assesses those risks independently from the business line, and an independent compliance function that monitors compliance with Applicable Law and standards.

Finally, there may be a review or audit function that provides independent review of, among other things, internal control systems and the activities of the business unit and the risk management and compliance functions.

Periodic independent reviews of risk and compliance controls should also be undertaken, including a review of the qualitative and quantitative assumptions within the risk management system.

The principles below describe numerous recommendations that illustrate how to achieve robust frameworks for risk management, compliance, and review. However, not every recommendation may be appropriate for every Market Participant. Accordingly, Market Participants should assess which

recommendations are appropriate based on the size and complexity of their Cryptoasset market activities, and the nature of their engagement in the Cryptoasset market, taking into account Applicable Law.

PRINCIPLE 27

Market Participants should have frameworks for risk management and compliance.

The common components of these two frameworks may include:

- Effective oversight by the senior body or individual(s), consistent with Principle 4, including support for the stature and independence of risk management and compliance. In particular:
  - ✓ the senior body or individual(s) should make strategic decisions on the risk appetite of the Cryptoasset business. The risk appetite for the Cryptoasset business should be reviewed periodically. When setting the risk appetite, Market Participants should take into consideration both normal and stress market conditions.
  - ✓ the senior body or individual(s) should be responsible for the establishment, communication, enforcement, and regular review of a risk management and compliance framework that clearly specifies authorities, limits, and policies. Risks should be managed prudently and responsibly in accordance with established principles of risk management and Applicable Law.
- The provision of concise, timely, accurate, and understandable risk and compliance related information to the senior body or individual(s).
- The appropriate segregation of duties and independent reporting lines, including the segregation of trading from risk management and compliance and from deal processing, accounting, and settlement. While risk managers and compliance personnel may work closely with business units, the risk management and compliance functions should be independent of the business unit and should not be directly involved in revenue generation. Compensation structures should be designed not to compromise such independence.
- Adequate resources and employees with clearly specified roles, responsibilities, and authority, including appropriate access to information and systems. These personnel should have appropriate knowledge, experience, and training.

PRINCIPLE 28

Market Participants should familiarize themselves with, and abide by, all Applicable Law and Standards that are relevant to their Cryptoasset Market activities and should have an appropriate compliance framework in place.

An effective compliance framework should provide independent oversight and control and could comprise, but is not limited to:

- identification of Applicable Law and standards that apply to their Cryptoasset Market activities;
- appropriate processes designed to detect, prevent, respond, and recover from abusive, collusive, or manipulative practices, fraud, and financial crime, and to mitigate material risk that could arise in the general conduct of the Cryptoasset Market activities;
- capturing and retaining adequate records to enable effective monitoring of compliance with Applicable Law and standards;
- well-defined escalation procedures for issues identified;
- consideration of the need to periodically restrict relevant personnel's access through measures such as mandatory vacation to facilitate detection of possible fraudulent activities;

- the provision of advice and guidance to senior management and personnel on the appropriate implementation of Applicable Law, standards, and other relevant guidance in the form of policies and procedures and other documents such as compliance manuals and internal codes of conduct;
- training and/or attestation processes to promote awareness of and compliance with Applicable Laws and standards;
- appropriate implementation and utilization of compliance programs (for example, the establishment of processes to monitor daily activities and operations, which may be 24/7/365); and
- the periodic review and assessment of compliance functions and controls, including mechanisms to alert senior management about material gaps or failures in such functions and controls. The appropriate senior body or individual(s) should oversee the timely resolution of any issues.

PRINCIPLE 29

Market Participants should maintain an appropriate risk management framework with systems and internal controls to identify and manage the Cryptoasset risks they face.

Effective risk management starts with the identification and understanding by Market Participants of the various types of risks to which they are exposed (see the section on Key Risk Types below), and typically involves the establishment of risk limits and monitoring mechanisms, as well as the adoption of risk-mitigating and other prudent practices. An effective risk management framework could comprise, but is not limited to:

- an appropriate and well-documented approval process for the setting of risk limits;
- Risk limits are to be reviewed periodically and are set to be consistent with business strategy, risk appetite and time to exit a comprehensive and well-documented strategy for the identification, measurement, aggregation, and monitoring of risks across the Cryptoasset business documented policies, procedures, and controls, which are periodically reviewed and tested, to manage and mitigate risks;
- the clear communication of risk management policies and controls within the institution to promote awareness and compliance, as well as processes and programs to facilitate the understanding of such policies and controls by personnel;
- information systems to facilitate the effective monitoring and timely reporting of risks;
- robust incident management, including appropriate escalation, mitigating actions, work around solutions, and lessons learned;
- robust risk assessment for all (and approval processes for new) products, services, and procedures to identify new or emerging risks;
- sound accounting policies and practices encompassing prudent and consistent valuation methods and procedures; and
- an appropriately robust risk control self-assessment process that includes processes to remediate identified gaps or weaknesses.

PRINCIPLE 30

Market Participants should have practices in place to limit, monitor, and control the risks related to their Cryptoasset Market trading activity.

These practices could comprise, but are not limited to:

- The regular monitoring of trading activities, including the identification and internal escalation, as appropriate, of failed, cancelled, or erroneous trades.

- Automated or manual monitoring systems to detect actual or attempted market misconduct and market manipulation. Relevant personnel should be qualified to detect trading patterns that may suggest unfair or manipulative practices. Market Participants may use certain statistics or metrics to flag behavior warranting further review, such as off-market rates, repetitive orders, and unusually small or large orders. There should be appropriate processes whereby suspicious practices can be promptly reviewed and escalated as appropriate.
- Verification of the valuations used for risk management and accounting purposes, conducted by personnel independent of the business unit that owns the risk.
- Independent reporting on a regular and timely basis of risk positions and trader profit/loss statements to the relevant risk management function or senior management, as appropriate, including a review of exceptional deviations of profit/loss from expected levels.
- Transactions should be promptly and accurately captured so that risk positions can be calculated in an accurate and timely manner for monitoring purposes (see Principle 45).
- Regular reconciliations of front, middle, and back office systems, with differences identified and their resolution tracked by personnel independent of the business unit.
- Timely reporting to a senior body or individual(s) when risk limits have been breached, including follow-up action to bring exposures within limits, and any appropriate measures to prevent a recurrence.
- Appropriate controls around proper order and quote submission, such as kill switches or throttles in the case of electronic trading submissions. These controls should be designed to prevent the entry or transmission of erroneous orders or quotes that exceed pre-set size and price parameters as well as financial exposure thresholds.

Market Participants should be aware of the risks associated with reliance on a single source of liquidity and incorporate contingency plans as appropriate.

PRINCIPLE 31

Market Participants should have processes in place to independently review the effectiveness of and adherence to the risk management and compliance functions.

Independent review should be performed regularly, with any review findings recorded and corrective action tracked.

All material risk related to Cryptoasset Market activities should be covered, using an appropriate assessment methodology.

The review team should be given the necessary mandate and support, including adequate personnel with requisite experience or expertise.

Findings should be reported to an appropriately senior level for review and follow-up.

The above may be undertaken by the audit function where appropriate.

II. Key Risk Types

Market Participants may be subject to different risks, and to varying degrees, depending on the size and complexity of their Cryptoasset market activities, and the nature of their engagement in the Cryptoasset market. With this in mind, the principles below outline some of the good practices relevant to the key risk types applicable to Cryptoasset activities.

Key Risk Types are categorized into Financial and Non-Financial Risks.

Financial Risks

CREDIT RISK

PRINCIPLE 32

Market Participants should have adequate processes to manage credit risk exposure, including where appropriate, through the use of credit limit monitoring processes and systems.

Market Participants should ensure they take measures to manage the credit risks they face to Cryptoasset issuers, exchanges, and intermediaries that custody such assets. Market participants should conduct a credit risk assessment and institute credit limits in an effective monitoring program. Market Participants should incorporate this key risk in all strategic business planning efforts.

COUNTERPARTY CREDIT RISK

PRINCIPLE 33

Market Participants should have adequate processes to manage counterparty credit risk exposure, including where appropriate, through the use of appropriate netting and collateral arrangements, such as legally enforceable master netting agreements and credit support arrangements.

The use of master netting agreements and credit support arrangements can help strengthen the smooth functioning of the Cryptoasset Market. Other measures to manage counterparty credit risk include the accurate and timely assessment of a counterparty's creditworthiness prior to a transaction, sufficient diversification of counterparty exposure where appropriate, the prompt setting and monitoring of counterparty exposure limits, and the acceptance of transactions only if they fall within approved limits. Credit limits should be set independently of the front office, and should reflect the established risk appetite of the Market Participant.

Market Participants should maintain accurate records material of their counterparty relationships. This could include records of conversations and written correspondence, and retention policies should be aligned with Applicable Law.

Cryptoasset Trading Venues that have multiple liquidity providers and consumers should at a minimum disclose the following as it relates to credit monitoring:

- what mechanisms and/or controls are in place to set, amend, and monitor all applicable credit limits;
- whether and how the responsibility of monitoring credit limit breaches falls upon the platform or the users, and which parties are responsible for resolving credit limit breaches; and
- what specific methodologies are used to calculate credit exposures (such as Net Open Position, etc.)

MARKET RISK

PRINCIPLE 34

Market Participants should have processes to measure, monitor, report, and manage market risk in an accurate and timely way.

Changes in Cryptoasset prices give rise to market risk, which could have an adverse effect on the financial condition of Market Participants. Market risk measurement should be based on generally accepted measurement techniques and concepts, including the use of stress testing. Such measurement techniques should be periodically and independently reviewed. The measurement of market risk should take into account hedging and diversification effects.

Market Participants should be aware of, monitor, and—where appropriate—mitigate the liquidity risk that could arise from their transactions in the Cryptoasset Market.

PRINCIPLE 35

Market Participants should have independent processes in place to mark-to-market trading positions to measure the size of their profit and loss and the market risk arising from trading positions.

In marking-to-market trading positions, quoted market prices, where available, are generally the best guide. When obtaining external data for valuation purposes:

- useful sources of data include screen services, brokers, and other third-party providers;
- a function independent of the front office should check that prices and marked-to-market valuations are measured accurately and regularly;
- there should be understanding of what the data represent—for example, if the price was the last actual trade, when the last trade was executed, and if prices were not actual trades how these were calculated.

Market Participants should have an internal agreed close of business for each trading day against which end-of-day positions can be monitored and evaluated.

Where reference market prices are not available (for example, in marking-to-market complex derivatives or exotic instruments), internal models, validated by an internal function that is independent from the front office, can be used to guide the appropriate pricing of risks.

FUNDING LIQUIDITY RISK

PRINCIPLE 36

Market Participants should have appropriate processes in place to monitor and manage their capacity to fund their positions and operations through different economic environments and ensure they can carry out their Principal business activities.

Market Participants should take into consideration key funding liquidity risks. Such risks may lead a firm to defaulting on its obligations and becoming insolvent. Funding liquidity risks can be driven by periods of high volatility in underlying Cryptoasset Markets.

Market participants should establish adequate capital reserves and stable funding profiles whilst maintaining robust monitoring and control processes to ensure their funding liquidity risk is well managed. Market Participants should also be aware of the risks associated with reliance on a single source of liquidity and incorporate contingency plans as appropriate.

Non-Financial Risks

OPERATIONAL RISK

PRINCIPLE 37

Market Participants should have appropriate processes in place to identify and manage operational risks that may arise from human error, inadequate or failed systems or processes, or external events.

Market Participants should take into consideration operational risks arising from a global cross-border environment, such as time differences or differences in industry conventions. Operational risks could include those arising from human error, misconduct, systems issues, or unforeseen external circumstances.

Market Participants should put in place strict security measures to address the vulnerability of trading areas and infrastructure to possible operational disruptions, terrorism, or sabotage. Access to the dealing function should be controlled, with procedures in place that specify time constraints, security checks, and management approvals around access, where appropriate, for non-dealing personnel and external visitors. The technology landscape for Cryptoassets poses unique cyber threats as well as challenges associated with the fact that inventory may be exchanged at all hours.

PRINCIPLE 38

Market Participants should have business continuity plans (BCPs) and IT disaster recovery plans in place that are appropriate to the nature, scale, and complexity of their Cryptoasset business and that can be implemented quickly and effectively in the event of large-scale disasters, loss of access to significant Trading Venues, settlement, or other critical services, or other market disruptions.

BCPs could comprise, but are not limited to, the following elements:

- Contingency plans that support business continuity across the Cryptoasset business, including plans related to data storage and usage, and procedures in the event of the non-availability of Cryptoasset fixes, where relevant.
- The regular review, updating, and testing of contingency plans, including drills to familiarize senior management and relevant personnel with the arrangements under a contingent situation. This should include the regular review of potential scenarios that would require the activation of such plans.
- Disaster recovery plans that identify requisite systems and procedural backups. All critical automated processes as determined by the Market Participant should have a documented automated and/or manual contingency.
- The identification of external dependencies, including an understanding of the BCPs of settlement system operators and other infrastructure and critical service providers, as well as the appropriate inclusion of these plans, or other back-up processes, into Market Participants' own BCPs.
- Emergency contact information for both internal and external dependencies. Communication tools should be secure.
- Non-primary location backup sites that can accommodate essential personnel, systems, and operations, and that are maintained and tested on a regular basis.

PRINCIPLE 39

Market Participants should have appropriate processes in place to manage the risks posed by engaging with third-party entities in any operational capacity.

Market Participants should conduct a periodic risk assessment including periodic due diligence review considering the threat each third party engaged in its operations poses.

Third-party service providers in the Cryptoasset Market face many of the same risks as their Clients and thus should be monitored closely.

PRINCIPLE 40

Market participants should manage their Settlement Risk by conducting a comprehensive review of its settlement processes and technologies leveraged to transfer value.

Market Participants should have documented policies, procedures, and processes in place to define settlement for different Cryptoassets and manage confirmation and risk.

Settlement can include the transfer or delivery of fiat currencies and Cryptoassets as well as on-chain minting or burning of Cryptoassets based on the nature of the Market Participant's transaction.

TECHNOLOGY RISK

PRINCIPLE 41

Market Participants should have in place processes to address potential adverse outcomes arising from the use of or reliance on technological systems (hardware and software).

Market Participants should have processes in place to assign clear ownership of every system on which they rely, and changes should be approved according to internal policies. Any system or critical piece of technology should be thoroughly reviewed for soundness and tested before release into production use, with an audit trail of all actions taken saved and available for review. This should apply to the development, testing, deployment, and subsequent updates of trading systems and algorithms.

Market Participants involved in electronic trading should put in place appropriate and proportionate controls to reduce the likelihood of and mitigate any consequences of generating or acting upon electronic quotations that may result in erroneous transactions or market disruption such as off-market quotes or trades, fat finger errors, unintended or controlled trading activity arising from technological failures, flaws in trading logic, and unexpected or extreme market conditions.

PRINCIPLE 42

Market Participants should have processes in place to address the unique cyber security risks it faces engaging in the Cryptoasset Market.

Market Participants should have processes in place to detect, prevent, respond, and recover from cyber security risks present in the Cryptoasset space.

PRINCIPLE 43

Market Participants should have processes in place to address protocol risks which can impact the usability and value of digital assets on associated blockchains.

Market Participants should prepare to address issues resulting from protocol risks by conducting a careful evaluation of the protocols and establishing policies and decision-making mechanisms to mitigate these risks. These policies may vary between native assets (e.g., bitcoin) versus tokenized assets (e.g., fiat-backed stablecoins).

Market Participants should establish rules for protocol changes in the agreements (e.g., establish rules for determining the reference Cryptoasset in the event of a protocol hard fork).

PRINCIPLE 44

Market Participants should have processes in place to address smart contract risks and technical vulnerabilities by conducting careful evaluations and audits.

Market Participants should mitigate the risk posed by smart contracts by conducting comprehensive audits of underlying technologies and instituting associated controls.

Just like any other software, smart contracts may have technical vulnerabilities and should be subject to careful evaluation and audit. In some cases, there may exist parties with administrative privileges over these contracts to override the business logic in part or in whole.

COMPLIANCE RISK

PRINCIPLE 45

Market Participants should keep a timely, consistent, and accurate record of their market activity to facilitate appropriate levels of transparency and auditability and have processes in place designed to prevent unauthorized transactions.

Market Participants should keep an accurate and timely record of orders and transactions that have been accepted and triggered/executed, as well as the reasons behind electronic trade request and order rejections, consistent with those set out under Principle 11, to create an effective audit trail for review and to provide transparency to Clients where appropriate.

This record may include, but is not limited to, the following: the date and time, product type, order type (for example, a Stop Loss Order, or an order where price is subject to last look), quantity, price, trader, and Client identity. Market Participants should apply sufficiently granular and consistent time-stamping so that they record both when an order is accepted and when it is triggered/executed.

Market Participants should have processes in place to support appropriate related data storage and retention of such detail.

Information should be made available to Clients upon request, to provide sufficient transparency regarding their orders and transactions to facilitate informed decisions regarding their market interactions. Information may also be used in resolving trade disputes. Records should allow Market Participants to effectively monitor their own compliance with internal policies, as well as their adherence to appropriate market behavior standards.

Market Participants should set guidelines that specify personnel authorized to deal in after-hours or off-premise transactions and the limit and type of transactions permitted. A prompt written reporting process should be developed and appropriate records should be kept.

PRINCIPLE 46

Market Participants should perform "know-your-customer" (KYC) checks on their counterparties to ascertain that their transactions are not used to facilitate money laundering, terrorist financing, or other criminal activities.

Market Participants should have appropriate measures in place to enforce the KYC principle (see Principle 62 in Confirmation and Settlement section).

Market Participants should have a clear understanding of all Applicable Law on the prevention of money laundering and terrorist financing.

Market Participants should have internal processes in place to facilitate the prompt reporting of suspicious activities (for example, to the compliance officer or appropriate public authority, as necessary). Effective training should be provided for relevant personnel, to raise awareness of the serious nature of these activities, and reporting obligations, while not revealing their suspicions to the entity or individual suspected of illegal activities. Such training should be regularly updated to keep pace with the rapidly changing methods of money laundering.

PRINCIPLE 47

Market Participants should have in place reasonable policies and procedures (or governance and controls) such that trading access, either direct or indirect, is limited to authorized personnel only.

Market Participants should maintain trader or desk mandates, which detail what products each trader is permitted to trade, as well as post-trade surveillance in order to detect exceptions from the trader's mandate.

Market Participants should periodically review trading access in order to confirm that such access, either direct or indirect, is limited to authorized access only.

Market Participants should implement monitoring practices designed to detect the concealment or manipulation of (or the attempt to conceal or manipulate) profit and loss and/or risk using trades or adjustments that are not for a genuine business purpose.

PRINCIPLE 48

Market Participants should generate a timely and accurate record of transactions undertaken to enable effective monitoring and auditability.

At the request of a Client, Market Participants should be able to provide information regarding the actions taken in handling a specific transaction with such Client. Clients requesting data from a Market Participant are expected to do so in a reasonable manner, avoiding spurious or extraneous requests. When requesting data, a Client should outline the reason for the request. Market Participants should have processes in place to respond to Client requests for the data.

LEGAL RISK

PRINCIPLE 49

Market Participants should have processes in place to identify and manage legal risks arising in relation to their Cryptoasset Market activities.

Market Participants should have an understanding of where Applicable Law may affect the legality or enforceability of rights and obligations with other Market Participants and should take steps to mitigate material legal risks. Given the nascent nature of Cryptoassets, there are many legal risks related to uncertainties in how such assets will be governed. Laws differ significantly across jurisdictions. Market Participants should have governance procedures in place to address risks associated with legal considerations such as ownership, transfer, settlement, remedies, and insolvency, among others.

Market Participants should have in place legal agreements with their counterparties, and should use standard terms and conditions, where appropriate. Market Participants should maintain a record of the agreements they have in place with their counterparties.

When trading, Market Participants should make clear if standard terms are used, and if changes are proposed. Where changes are substantial, these should be agreed before any transaction. Where standard terms do not exist, Market Participants should take more care in the negotiation of these terms. Market Participants should strive to finalize documentation promptly.

REGULATORY RISK

PRINCIPLE 50

Market Participants should monitor the various jurisdictions in which they transact in Cryptoassets to ensure the appropriate registrations, licenses, and regulatory compliance programs are in place.

Market participants should recognize that regulations and requirements to transact in Cryptoassets can vary across jurisdictions, which may include, but are not limited to money transmitter licenses, securities dealer or exchange licenses, and commodities exchange licenses.

CONSIDERATIONS RELATED TO PRIME BROKERAGE ACTIVITIES

PRINCIPLE 51

Prime brokerage participants should strive to monitor and control trading permissions and credit provision in Real Time at all stages of transactions in a manner consistent with the profile of their activity in the market to reduce risk to all parties.

Prime Brokerage Participants should strive to develop and/or implement robust control systems that include the timely allocation, monitoring, amendment, and/or termination of credit limits and permissions and adequately manage associated risks.

Prime brokerage clients should strive for Real-Time monitoring of their available lines and permitted transaction types and tenors so that only trades within permitted parameters are executed.

Executing dealers should strive for Real-Time monitoring of designation limits to validate trade requests prior to execution.

Prime Brokers should have systems reasonably designed to monitor trading activity and applicable limits upon receiving Give-Up trades.

Prime Brokers should be in a position to accept trades in accordance with terms and conditions within Prime Brokerage agreements and designation notices.

Prime Brokers should have policies and procedures reasonably designed to address limit breach exceptions, limit changes, amendments, and novations.

Prime Brokers should clearly disclose to Clients how they monitor their credit limits and how limit breaches are managed.

Confirmation and Settlement

LEADING PRINCIPLE:

Market Participants are expected to put in place robust, efficient, transparent, and risk-mitigating post-trade processes to promote the predictable, smooth, and timely settlement of Cryptoasset transactions.

The principles below relate to systems and processes surrounding the confirmation and settlement of Cryptoasset trades. These principles should be applied in a manner consistent with the size and complexity of the Market Participant's Cryptoasset Market activities, and the nature of its engagement in the Cryptoasset Markets.

I. Overarching Principles

PRINCIPLE 52

Market Participants should establish consistency between their operating practices, their documentation, and their policies for managing credit and legal risk.

Operating practices (including processes for confirming and settling trades) should be well documented and consistent with the legal terms of the transaction. Similarly, the use of mitigants for credit risk should be consistent with this documentation and with the Market Participant's credit risk policies.

PRINCIPLE 53

Market Participants should institute a robust framework for monitoring and managing capacity of transaction, settlement, deposit, and withdrawal volumes in both normal and stressed market conditions.

At a minimum, Market Participants should have sufficient technical and operational capability to support end-to-end Cryptoasset processing in both normal and stressed market conditions without undue impact on the processing timeline. Operational guidelines should include considerations for on-chain settlement criteria (e.g., two confirmations on Bitcoin).

Market Participants should have defined mechanisms in place to respond to extreme changes in demand, as required and on a timely basis. Furthermore, clearly defined and documented capacity and performance management processes should be in place and reviewed regularly, including with external vendors.

PRINCIPLE 54

Market Participants are encouraged to implement straight-through automatic transmission of trade data from their front office systems to their operations systems and relevant blockchain protocols.

Such transfer of trade data should be facilitated by means of secure interfaces where the transmitted trade data cannot be changed or deleted during transmission. Confirmation that third-party technological audit(s) have been undertaken to verify that the technology and code works as intended and that it is secure. When trade data cannot be transmitted automatically from the front office to the operations system, adequate controls should be in place so that trade data are captured completely and accurately in the operations system.

PRINCIPLE 55

Market Participants should conduct any novations, amendments, and/or cancellations of transactions, where applicable, in a carefully controlled manner.

Processes for novating, amending, or cancelling transactions should be clearly defined and should provide for the maintenance of appropriate segregation between operations and sales and trading personnel. Reporting on amendments and cancellations should be made available to management in these areas on a regular basis.

II. Confirmation Process

PRINCIPLE 56

Market Participants should confirm trades as soon as practicable, and in a secure and efficient manner.

Market Participants should confirm Cryptoasset trades as soon as practicable after execution, amendment, or cancellation. The use of automated trade confirmation matching systems, when available, is strongly recommended. Market Participants should also implement operating practices that segregate responsibility for trade confirmation from trade execution.

Market Participants should be efficient and effective in meeting obligations in respect of the services they provide in a timely manner. They should make use of relevant market standards and procedures to facilitate efficient settlement and to meet applicable recording requirements.

Confirmations should be transmitted in a secure manner whenever possible, and electronic and automated confirmations are encouraged. When available, standardized message types and industry-agreed templates should be used to confirm Cryptoasset products. Trades arranged via an over-the-counter (OTC) desk should be confirmed directly between both parties to the transaction. Market Participants should receive an affirmation from the OTC desk to assist in accurately booking trades.

Open communication methods such as e-mail can significantly increase the risk of fraudulent correspondence or disclosure of Confidential Information to unauthorized parties. If confirmations are communicated via open communication methods, those methods should comply with information security standards (and also see Principle 25 in Information Sharing).

If Market Participants bilaterally choose to match trades using front-end electronic dealing platforms in place of exchanging traditional confirmation messages, the exchange of trade data should be automated and flow straight-through from the front-end system to operations systems. Strict controls should be in place so that the flow of data between the two systems is not changed and that data are not deleted or manually amended. Any agreements between the parties to use electronic dealing platforms for trade matching rather than exchanging traditional confirmation messages should be documented in the legal agreement between the parties.

PRINCIPLE 57

Market Participants should review, affirm, and allocate block transactions as soon as practicable.

Block transaction details should be reviewed and affirmed as soon as practicable following execution. Investment managers or others acting as Agent on behalf of multiple counterparties may undertake block transactions that are subsequently allocated to specific underlying counterparties. Each underlying counterparty in a block transaction should be an approved and existing counterparty of the dealer-counterparty prior to allocation. Each post-allocation transaction should be advised to the counterparty and confirmed as soon as practicable.

PRINCIPLE 58

Market Participants should identify and resolve confirmation and settlement discrepancies as soon as practicable.

Market Participants that identify discrepancies between received confirmations or alleged trades and their own trade records should investigate internally and inform their counterpart with the aim to resolve such discrepancies as soon as practicable. Market Participants should also carefully reconcile all alleged trades and inform senders of unknown confirmations that the recipient cannot allocate to any internal trade record.

Escalation procedures should be established to resolve any unconfirmed or disputed terms as a matter of urgency, and processes should be in place to detect and report adverse trends that emerge in the discrepancies. Escalation procedures should also include notification to trading and other relevant internal parties so that they know which counterparties may have practices that do not align with best practices regarding confirmation of trades. Senior management should receive regular information on the number and latency of unconfirmed deals so that they can evaluate the level of operational risk being introduced by maintaining dealing relationships with their firms' counterparties.

PRINCIPLE 59

Market Participants should be aware of the particular confirmation and processing features specific to life cycle events of each Cryptoasset product and associated derivatives.

Market Participants should establish clear policies and procedures for the confirmation, exercise, and settlement of all Cryptoasset products and their derivatives in which they transact, including those with unique features. Where applicable, Market Participants should familiarize personnel responsible for operations with the additional terms and conditions associated with various Cryptoasset products and the protocols and processes around life cycle events in order to reduce operational risk. Market Participants should also be fully versed in the appropriate terminology, contract provisions, and market practices associated with Cryptoasset products. Counterparties should agree on a common definition of events that may take place during the lifecycle of transactions, including treatment of forks in the network of the underlying asset and airdrops associated with the network of the underlying asset.

III. Netting and Settlement Processes

PRINCIPLE 60

Market Participants should properly measure, monitor, and control their Settlement Risk equivalently to other counterparty credit exposures of similar size and duration.

Where PVP settlement is not used, Settlement Risk should be properly measured, monitored, and controlled. Market Participants should set binding ex ante limits and use controls equivalent to other credit exposures of similar size and duration to the same counterparty. When a decision is made to allow a Client to exceed a limit, appropriate approval should be obtained.

Where settlement amounts are to be netted, the initial confirmation of trades to be netted should be performed as it would be for any other Cryptoasset transaction. All initial trades should be confirmed before they are included in a netting calculation. In the case of bilateral netting, processes for netting settlement values used by Market Participants should also include a procedure for confirming the bilateral net amounts in each Cryptoasset or fiat currency at a predetermined cut-off point that has been agreed upon with the relevant counterparty.

To avoid underestimating the size and duration of exposures, Market Participants should recognize that Settlement Risk exposure to their counterparty begins when a payment order on the Cryptoasset or fiat currency it sold can no longer be recalled or cancelled with certainty, which may be before the settlement date. Market Participants should also recognize that funds might not have been received until it is confirmed that the trade has settled with finality during the reconciliation process.

PRINCIPLE 61

Market Participants should utilize standing settlement instructions (SSIs).

SSIs for all relevant products and currencies should be in place, where practicable, for counterparties with whom a Market Participant has a trading relationship. The responsibility for entering, authenticating, and maintaining SSIs should reside with personnel clearly segregated from a Market Participant's trading and sales personnel and ideally from those operational personnel responsible for trade settlement. SSIs should be securely stored and provided to all relevant settlement systems so as to facilitate straight-through processing. The use of multiple SSIs with the same counterparty for a given Cryptoasset or fiat

currency is discouraged. Because of the Settlement Risks it introduces, the use of multiple SSIs with the same counterparty for a given Cryptoasset or fiat currency should have appropriate controls.

SSIs should be set up with a defined start date and captured and amended (including audit trail recording) with the appropriate approvals, such as review by at least two individuals. Counterparties should be notified of changes to SSIs with sufficient time in advance of their implementation. Changes, notifications, and new SSIs should be delivered via an authenticated, and standardized, message type whenever possible.

All transactions should be settled in accordance with the SSIs in force on the value date. Trades that are outstanding at the time SSIs are changed (and have a value date on or after the start date for the new SSIs) should be reconfirmed prior to settlement (either bilaterally or through an authenticated message broadcast).

Where SSIs are not available (or existing SSIs are not appropriate to the particular trade), the alternate settlement instructions to be used should be delivered as soon as practicable. These instructions should be exchanged via an authenticated message or other secure means and subsequently verified as part of the trade confirmation process.

PRINCIPLE 62

Market Participants should request Direct Payments.

Market Participants should request Direct Payments when conducting Cryptoasset transactions and recognize that Third-Party Payments may significantly increase operational risk and potentially expose all parties involved to money laundering or other fraudulent activity. Market Participants engaging in Third-Party Payments should have clearly formulated policies regarding their use and any such payments should comply with such policies.

At a minimum, these policies should require the payer to be furnished with a clear understanding of the reasons for Third-Party Payments and for risk assessments to be made in respect of anti-money laundering, counter-terrorism financing, and other Applicable Law. Arrangements for Third-Party Payments should also be agreed upon and documented between the counterparties prior to trading. In the event a Third-Party Payment is requested after a trade has been executed, the same level of due diligence should be exercised and relevant compliance and risk approvals should be sought and secured.

PRINCIPLE 63

Market Participants should have adequate systems in place to allow them to project, monitor, and manage their intraday and end-of-day funding requirements to reduce potential complications during the settlement process.

Market Participants should appropriately manage their funding needs and ensure that they are able to meet their Cryptoasset and fiat currency payment obligations on time. A Market Participant's failure to meet its Cryptoasset and fiat currency payment obligations in a timely manner may impair the ability of one, or more, counterparties to complete their own settlement, and may lead to liquidity dislocations and disruptions in the payment and settlement systems.

Market Participants should have clear procedures outlining how each of their accounts used for the settlement of Cryptoasset transactions is to be funded. Whenever possible, those Market Participants with

nostro accounts and/or custodians should be projecting the balance of these accounts on a Real-Time basis, including all trades, cancellations, and amendments for each tenor (value date) so that they can diminish the overdraft risk from the nostro account.

Market Participants should send payment instructions as soon as practicable, taking into consideration time zone differences as well as instruction receipt cut-off times imposed by their correspondents. Market Participants should communicate expected receipts (via standardized message types, when possible) to allow nostro banks to identify and correct payment errors on a timely basis and aid in the formulation of escalation procedures.

Market Participants should communicate with their custodians and nostro banks to process the cancellations and amendments of payment instructions. Market Participants should understand when they can unilaterally cancel or amend payment instructions and should negotiate with their nostro banks to make these cut-off times as close as possible to the start of the settlement cycles agreed with their counterparties.

IV. Account Reconciliation Processes

PRINCIPLE 64

Market Participants should perform timely account reconciliation processes.

Market Participants should conduct a regular reconciliation process to reconcile expected Cryptoasset and fiat currency flows against actual flows on a timely basis. The sooner reconciliations are performed, the sooner a Market Participant can detect missing or erroneous entries and know its true account balances so that it can take appropriate actions to confirm that its accounts are properly funded. Reconciliations should be carried out by personnel who are not involved in processing transactions that would affect the balances of accounts held with correspondent banks and/or custodians.

Full reconciliation should occur across custodians and nostro accounts as early as possible. To aid in the full reconciliation of their custodians and nostro accounts, Market Participants should be capable of receiving automated feeds of custodial and nostro activity statements and implement automated custodian and nostro reconciliation systems. Market Participants should also have measures in place to resolve disputes.

Escalation procedures should be in place and initiated to deal with any unreconciled Cryptoasset and fiat currency balances and/or unsettled trades.

PRINCIPLE 65

Market Participants should identify settlement discrepancies and submit compensation claims in a timely manner.

Market Participants should establish procedures for detecting non-receipt of payments, late receipt of payments, incorrect amounts, duplicate payments, and stray payments and for notifying appropriate parties of these occurrences. Escalation procedures should be in place for liaising with counterparties that fail to make payments and more broadly for the resolution of any disputes. Escalation should also be aligned to the commercial risk resulting from fails and disputes. Market Participants that have failed to make a payment on a value date or received a payment in error (for example, a stray payment or duplicate payment) should arrange for proper value to be applied or pay compensation costs in a timely manner.

All instances of non-receipt of payment should be reported immediately to the counterparty's operations and/or trading units. Market Participants should update their settlement exposure with the most recent projected cash flow movements. Market Participants may wish to consider a limited dealing relationship with counterparties that have a history of settlement problems and continue to fail on their payments.

ANNEX 1:

Illustrative Examples

The examples provided in the Standards are intended to illustrate the principles and situations in which the principles could apply. The examples are highly stylized and are not intended as, nor should be understood or interpreted as, precise rules or prescriptive or comprehensive guidance. Moreover, the examples are not intended to provide safe harbor nor are they an exhaustive list of situations that can arise; in fact, it is expressly understood that facts and circumstances can and will vary. In some examples, specific market roles are used to make the example more realistic but the illustrated behavior applies to all Market Participants.

The examples are grouped under leading principles based on the key principle that is being illustrated. However, in many cases a number of leading principles may apply to each illustrated example. Examples marked by an "**X**" illustrate conduct to be avoided; examples marked by a "check mark" illustrate conduct that the Standards aims to foster and reinforce. The Examples Annex can be expected to be updated over time as features of the Cryptoasset Market evolve.

Similar to other sections of the Standards, these illustrative examples should be interpreted by Market Participants in a professional and responsible manner. Market participants are expected to exercise sound judgement and to act in an ethical and professional manner.

EXECUTION

Market Participants should be clear about the capacities in which they act. (Principle 10)

- ✓ A Client asks a Market Participant to buy BTC on their behalf in the market. The Market Participant has an agreement with the Client stating it acts as an Agent and that the Market Participant will add a fee. The Market Participant executes the order in the market, showing a post trade execution analysis of the fills and adding the fee.

Market Participants should be clear about the capacities in which they act. In this example, the parties have made clear in advance the capacities in which they act and that the Market Participant would add a fee. Specifically, the Market Participant executes the Client's request in an agent capacity and is transparent about the nature of execution and the associated cost.

- ✓ A Client asks a Market Participant to buy BTC as a Market Order. The Market Participant and the Client have a Principal-based relationship, stipulated in their terms and conditions. The Market Participant fills the Client's order in accordance with the terms agreed, possibly using its own inventory and the available liquidity in the market.

Market Participants should be clear about the capacities in which they act. In this example, the parties have made clear in advance the capacities in which they act, by previously disclosing the terms and conditions under which it will interact with the Client. Specifically, the Market Participant and the Client, acting as Principals, agree to execute the transaction.

Market Participants should handle orders fairly and with transparency. (Principles 11 and 12)

- ✓ An OTC Desk receives a large order from a fund (Client) to sell 3-month BTC forwards at the Bitcoin Futures closing price. According to their pre-agreed terms and conditions, the OTC Desk and the Client have agreed that the OTC Desk will act as Principal and may hedge transactions depending on market conditions. The OTC Desk hedges some of the order amount before the CME closing since it judges there may not be sufficient liquidity in OTC markets after the closing to clear such a large amount without affecting the market rate to the Client's disadvantage. The OTC Desk keeps some of the risk on its book and does not trade the full amount in the market, therefore lessening the market impact of the Client's order following the CME closing, with the intention of benefiting the Client.

Market Participants are expected to handle orders with fairness and transparency. In this example, the Client and the OTC Desk have agreed that the latter will act as Principal. The OTC Desk executes the transaction in a manner that benefits the Client by lessening the market impact of the Client's order on the market.

- **X** A Market Participant has orders from several Clients to buy BTC. The Market Participant has disclosed to Clients its policy that electronic orders are processed in the order in which they are received from Clients. The Market Participant fills first an order of another customer even though that order was received after other orders.

Market Participants should make Clients aware of factors that affect how orders are handled and transacted, including whether orders are aggregated or time prioritized, and should have clear standards in place that strive for a fair and transparent outcome for the Client. In this example, the Market Participant has made the Client aware of its order-processing policy, but it violates that policy when it executes the orders in a non-sequential way.

- **X** A Client calls a Market Participant to execute a series of trades, stating that it is relying on the agency agreement they have in place. The agency agreement includes a pre-negotiated transaction fee. While executing the trades, the execution desk of the Market Participant adds an additional undisclosed spread to every trade it executes, resulting in the Client paying above the pre-negotiated transaction fee.

A Market Participant handling Client orders in an Agent role should be transparent with its Clients about its terms and conditions, which clearly set out fees and commissions. In this example, the Market Participant charges a fee in excess of the pre-negotiated fee and does not disclose it to the Client.

- **X** Dealer A tells Broker B that he has a large amount to execute at the Bitcoin Futures closing price and wants some help establishing a favorable rate to its benefit. Broker B then informs Dealer C who has a similar order and they all agree to combine their orders so as to make a greater impact before the Bitcoin Futures market closes.

Market Participants should handle orders fairly and with transparency, should not disclose confidential Client trading information (Principle 21, and should behave in an ethical and professional manner (Principles 1 and 2). The collusion illustrated in this example to intentionally influence a benchmark prices neither ethical nor professional. It divulges information about Client trading activity to an external party and is non-competitive behavior that undermines the fair and effective functioning of the Cryptoasset Market.

- ✓ A hedge fund calls an OTC Desk to buy a large amount of BTC by tomorrow morning, New York time. The Client and the bank agree that the OTC Desk will act as Principal and may hedge the transaction. Judging the liquidity not good enough to absorb the order, the OTC Desk starts to buy small parcels of BTC to limit the market impact of the transaction. The Desk fills the Client's order in the morning, using its inventory.

Market Participants should handle orders fairly and transparently. In this example, the Market Participant strives for a fair outcome for the Client.

- **X** A Client instructs a Market Participant to buy 10,000 BTC as part of its corporate treasury strategy. After receiving this instruction, but before executing the Client's order, the Market Participant buys 1,000 BTC for its own book, and not part of a risk management strategy for the transaction. After the settlement of the client order, the Market Participant sells 1,000 BTC for its own book, with the sole intent of taking advantage of the price movement caused by the Client order.

Market Participants should handle orders fairly and transparently, and the Confidential Information obtained from a Client is to be used only for the specific purpose for which it was given. In this example, the Market Participant instead uses its knowledge of the Client order and its expected market impact to gain profit for its own book, potentially disadvantaging the Client.

- ✓ A Market Participant is anticipating an order related to a potential merger and acquisition transaction on behalf of a Client that involves selling a very large amount of BTC. The Market Participant recognizes that this transaction could have a sizeable impact on the market and therefore proactively engages the Client to discuss a potential execution strategy, including but not limited to the matching of internal flows, the timing of the execution, the use of algorithms, and Pre-Hedging. The Market Participant transacts in anticipation of the order in agreement with the Client and with the intent to manage the risk associated with the anticipated transaction and to seek a better outcome for the Client.

Market Participants handling orders that have the potential to have sizable market impact should do so with care and attention. The order described in this example is large and could have sizable market impact and the parties involved take several steps to appropriately monitor and execute the order.

<u>A Market Participant should only Pre-Hedge Client orders when acting as a Principal, and should do so fairly and with transparency. (Principle 13)</u>

- ✓ A Market Participant has disclosed to a Client that the Market Participant acts as Principal and may pre-hedge the Client's anticipated order. The Client asks the Market Participant for a bid price for a large amount of BTC during a non-liquid period of the day. Due to liquidity conditions

and the size of the anticipated order, the Market Participant expects that it may need to quote a significantly lower bid than the current market price. But before determining its quote, and in an effort to improve its price to the Client, the Market Participant tests the market liquidity by selling a small amount ahead of providing a quote to the Client. The Market Participant quotes the Client a bid price for the full amount, taking into account, for the Client's benefit, the amount already sold.

Market participants should only Pre-Hedge anticipated Client orders when acting as a Principal and in a manner not meant to disadvantage the Client. In this example, the Market Participant has Pre-Hedged part of the order to manage the potential risk associated with the anticipated order and in a way intended to benefit the Client, specifically by taking into account the pricing benefit of the Pre-Hedged amount for the Client.

X A Client asks a Market Participant for a bid for 100 BTC. The Market Participant has disclosed to its Client that it acts as Principal and may Pre-Hedge the Client's anticipated orders. The bank then proceeds to sell 200 BTC in the market outside of their ongoing business before providing a bid, with the intent of taking advantage of the Client's trade request information and benefitting from a potentially lower market price.

Pre-Hedging is meant for the management of the risk associated with anticipated Client orders, designed to benefit the Client. Market Participants should only Pre-Hedge Client orders when acting as Principal. In this example, the amount intentionally sold by the Market Participant as a part of the Pre-Hedge was not commensurate with the risk borne by the anticipated trade and is not designed to benefit the Client. The bank acted with the intent to take advantage of the Client's trade request for its own benefit and potentially puts the Client at a disadvantage. A Market Participant should also consider prevailing market conditions and the size and nature of the anticipated transaction in assessing whether to Pre-Hedge the transaction.

Market Participants should not request transactions, create orders, or provide prices with the intent of disrupting market functioning or hindering price discovery. (Principle 14)

X A Market Participant wishes to sell a large amount of BTC. Before doing so, the Market Participant executes a number of small, successive purchases of BTC on a widely viewed Cryptoasset Trading Venue with the intention of moving the market price higher and inducing other Market Participants to buy BTC. The Market Participant then executes the original large sell order in one or more Cryptoasset Trading Venues at a higher price.

Market Participants should not request transactions or create orders with the intention of disrupting market functioning or hindering the price discovery process, including undertaking actions designed to result in a false impression of market price, depth, or liquidity. This example illustrates a strategy intended to cause artificial price movements. While Market Participants often break large trades into smaller transactions to mitigate the impact of a transaction, in this case the small transactions are intended to cause an artificial price movement. The Market Participant plans to sell a large quantity of currency but uses small buy trades to create a false impression of market price.

X A Market Participant wishes to sell a large amount of BTC. It repeatedly places small offers to sell on a widely viewed Cryptoasset Trading Venue. The Market Participant chooses to use another

dealing code of the same institution on the same Cryptoasset Trading Venue in order to lift these successive higher offers with the intention of misleading the market.

This is an extension of the previous example. The behavior gives the false impression that multiple counterparties are participating in a rally whereas they are actually from the same institution. The use of such strategies should be avoided.

X A Client stands to gain by moving the market higher into the 4:00 p.m. closing of the CME. They call an OTC Desk at 3:45 p.m. and place a large order and then instruct the bank to "buy the amount as quickly as possible". Market Participants should not request transactions or create orders with the intention of disrupting market functioning or hindering the price discovery process, including adopting strategies designed to result in a false impression of market price, depth, or liquidity. The Client's request in this example is intended to result in a false impression of market price and depth. Market Participants should understand how reference prices, including highs and lows, are established in connection with their transactions and/or orders. (Principle 15)

✓ A market maker discloses to a Client how reference prices will be established. After a sharp downward move in BTC, the market maker executes the Client's Stop Loss Order using a reference rate in accordance with its own policy and its prior disclosure.

Market Participants should understand how reference prices are established in connection with their transactions and orders. In this example, the market maker discloses to the Client how reference prices will be established.

<u>Mark Up should be fair and reasonable. (Principle 16)</u>

X A Market Participant receives a Client Stop Loss sell order for BTC at a certain level. When that level is traded in the market, the Market Participant executes the Stop Loss order with some slippage. However, the Market Participant fills the Client at a slightly lower rate after taking Mark Up and without having previously disclosed to the Client that the all-in price for executing a Stop Loss was subject to Mark Up.

Mark Up should be fair and reasonable, and Market Participants should promote transparency by disclosing to Clients that that their final transaction price may include Mark Up and that it may impact the pricing and execution of orders triggered at a specific level. In this example, the Market Participant has not disclosed to the Client how Mark Up will affect the all-in price for the order.

X A Market Participant charges a corporate higher markup than other corporates of the same size, credit risk, and relationship, exploiting the corporate's relative lack of sophistication in understanding and challenging the pricing of the Market Participant.

Mark Up should be fair and reasonable and can reflect a number of considerations, which might include risks taken, costs incurred, and services rendered to a particular Client, factors related to the specific transaction and to the broader Client relationship. The application of Mark Up in this example is not fair and reasonable as it discriminates between Clients based only on their level of sophistication. In the example below, the different Mark Up charged to each of the Clients is motivated by differences in the broader Client relationship—in this case, the volume of business.

- ✓ A Market Participant charges corporates of similar size and credit standing different Mark Ups because the broader Client relationship differs. For example, the volume of business these Clients transact with the Market Participant is of very different magnitudes.

Market Participants should identify and resolve trade discrepancies as soon as practicable to contribute to a well-functioning Cryptoasset Market. (Principle 17)

- **X** A hedge fund executes a trade through an executing Dealer for Give-Up to its Prime Broker (PB). The terms of the trade provided by the hedge fund to its PB do not match those provided by the executing Dealer. When notified by the PB that there is a discrepancy in the trade details, the hedge fund responds that the executing Dealer has made a mistake and that the PB should resolve the trade discrepancy with the executing Dealer.

Market Participants should resolve discrepancies as soon as practicable. In particular, Prime Brokerage Clients and executing dealers are responsible for resolving trade discrepancies to achieve timely amendments and matching of trade terms through the Prime Broker. In this example, the hedge fund places responsibility for resolving the discrepancy on the Prime Broker. However, it should have contacted the Dealer directly to resolve the discrepancy because the identities of the counterparties are known by the hedge fund and the executing dealer.

- ✓ A Client uses an Cryptoasset Trading Venue to execute Cryptoasset trades in the name of its Prime Broker. The Cryptoasset Trading Venue's rules do not allow the full name of the Executing Dealer whose orders match with the Client's orders to be revealed to the Client. The Cryptoasset Trading Venue confirms a trade at a price that differs from the Client's records. The Cryptoasset Trading Venue and Prime Broker work together with the Client to enable prompt resolution of the trade discrepancy. Specifically, the Cryptoasset Trading Venue contacts the executing dealer while maintaining confidentiality of the Client.

Market Participants should resolve trade discrepancies as soon as practicable and protect Confidential Information, as outlined in Principle 22. Where anonymous market access is provided, the access provider should assist in the resolution of trade discrepancies. In this example, while the Client and executing dealer are responsible for resolving the trade discrepancy, they do need help from the Prime Broker and the Cryptoasset Trading Venue because the Client and Executing Dealer do not know, and should not know, each other's name.

Market Participants employing last look should be transparent regarding its use and provide appropriate disclosures to Clients. (Principle 18)

- **X** A Market Participant sends a trade request to an anonymous liquidity provider to buy 10 BTC at a price of 20,000 USD via an Cryptoasset Trading Venue while the displayed price is 19,500 USD. This trade request is understood to be subject to a last look window before it is accepted and confirmed by the anonymous liquidity provider. During this window, the liquidity provider places buy orders at levels below the 19,500 USD price. If these buy orders are filled, the liquidity provider confirms and fills the Market Participant's trade request, but when these orders are not filled, neither is the Market Participant's trade request.

Market Participants should only use last look as a risk control mechanism to verify factors such as validity and price. In this example, the liquidity provider misuses the information contained in the Client's trade request to determine if a profit can be made and has no intent to fill the trade request unless a profit is possible.

- ✓ A Client sends trade requests that are subject to a last look window, and its liquidity provider has disclosed for what purposes last look may be used. The Client reviews data related to its average fill ratios on such transactions. The data provided suggests that its average fill ratio is lower than expected and the Client follows up with its liquidity provider to discuss reasons for this.

Market participants employing last look should be transparent regarding its use and provide appropriate disclosures to Clients. It is also good practice to be available to engage in a dialogue with Clients regarding how their orders have been handled. In this example, the Market Participant's transparency has enabled the Client to make an informed decision about how its orders are handled, and fosters dialogue between the two parties.

- **X** A Client requests to buy 21 BTC on a Cryptoasset Trading Venue. During the last look window, the Market Participant, taking into account the Client's request to trade, skews its pricing on Trading Venues higher.

Market Participants should not use the information contained in a Client's trade request during the last look window. In this example the Market Participant utilizes the information contained in the Client's trade request to change its prices on Cryptoasset Trading Venues during the last look window. By doing this, the Market Participant potentially signals to the market the interest of the Client, who then may be at a disadvantage were the Market Participant to subsequently reject the trade.

- ✓ A Client requests to buy 21 BTC with a Market Participant on an Cryptoasset Trading Venue. During the last look window associated with that trade request the Market Participant continues to update its prices for BTC and other Cryptoassets on a number of Cryptoasset Trading Venues. The prices the Market Participant shows on these platforms reflect normal inputs into the Market Participant's pricing algorithms, including movements in market prices and other transactions completed by the Market Participant, but does not use the information from the Client's request to trade as an input into those price changes during the last look window.

Market Participants may update pricing while a last look window remains open if the update is entirely independent of the relevant trade request, as doing so allows Market Participants to continuously make prices. Given the speed of electronic trading Market Participants will commonly need to update pricing while one or more last look windows remain open. In this example, the Market Participant takes no account of the trade request when updating pricing during the last look window.

- **X** A Client requests to sell 25 BTC with a Market Participant (OTC Desk A) at the price quoted to them by OTC Desk A. The Client makes their trade request on the understanding that OTC Desk A will not take on market risk in connection with the request and will only fill the request by first entering into offsetting transactions in the market. During the last look window, OTC Desk A sends a trade request to another Market Participant (its liquidity provider) to sell 25 BTC. This trade request is accepted by the liquidity provider. During the last look window, the market

moves lower. OTC Desk A fills their Client for 20 BTC, rather than for the full 25 BTC it transacted, rejecting the remaining 5 BTC. OTC Desk A closes out their remaining 5 BTC short position in the market at a lower price.

Market Participants that utilize the information from trade requests to conduct trading activity in the last look window should always pass on to their Client all volume that is traded in that period. In this example, the bank has not passed on to its Client the entirety of the volume that it traded in the last look window but has sought to take advantage of price movements to close out their position more profitably in the market.

Market Participants providing algorithmic trading or aggregation services to Clients should provide adequate disclosure regarding how they operate. (Principle 19)

X An aggregator preferentially routes an order to an Cryptoasset Trading Venue that provides brokerage rebates. The provider of the aggregator does not disclose to Clients that brokerage rebates affect routing preferences.

Market Participants providing aggregation services to Clients should provide adequate disclosure regarding how they operate, in particular general information regarding how routing preferences may be determined. In this example, the provider of the aggregator service has not disclosed a factor that determines routing preferences.

✓ A Client selects an OTC Desk's execution algo to buy 50 BTC. The OTC Desk markets this particular algo as being executed on a 'Direct Market Access' basis. The Client understands this means that the OTC's algo desk will select liquidity by looking across multiple sources, with the intention of delivering the highest possible execution quality available at that time to the Client. The OTC Desk further indicates that the algo may use internal liquidity. The OTC Desk has also disclosed how it manages the potential conflicts of interest arising from this dual role. After the order has been executed, the OTC Desk provides transparent post trade data, demonstrating the origin and price of each trade executed to fill the algo. In reviewing the post-trade data, the Client feels confident that the algo has selected the best liquidity available at the time of execution.

Market Participants should be clear about the capacities in which they act. Market Participants should handle orders fairly and with transparency in line with the capacities in which they act (Principle 11). Market Participants providing algorithmic trading or aggregation services to Clients should provide adequate disclosure regarding how they operate. Desks wishing to offer their own liquidity while operating algorithms should provide clear transparency of this practice through disclosure and manage any conflicts of interest that could impact the handling of the Client order. They should make available sufficient post-trade information to the Client, for the Client to verify that the algo always selected the best prices available either in the market, or against the OTC Desk's internal liquidity.

X A Client selects an OTC Desk's execution algo to buy 50 BTC. The OTC Desk markets this particular algo as being executed on a 'Direct Market Access' basis. The Client understands this means that the OTC Desk's algo desk will select liquidity by looking across multiple sources, with the intention of delivering the highest possible execution quality available at that time to the Client. The OTC Desk further indicates that the algo may use internal liquidity. However, the bank is not effectively managing the conflicts of interest that may arise from this dual role: the

market-making desk has sight of the parent order and the algo execution logic is pre-set to direct the last 10 BTC to the internal market-making desk with the intention of maximizing return.

Market Participants should handle orders fairly and with transparency in line with the capacities in which they act (Principle 11), and Market Participants providing algorithmic trading or aggregation services to Clients should provide adequate disclosure regarding how they operate. In this example, the OTC Desk has not fully disclosed how the algorithm works or managed the conflicts of interests in its dual role. It is using Confidential Information and prioritizing its own principal pricing over the market price.

INFORMATION SHARING

Market Participants should identify and protect Confidential Information. (Principles 21 and 22)

X Asset manager to a market maker: Market Participant ABC just called me with an Axe to buy BTC. Are you seeing buying as well?

Market Participants should not disclose or solicit Confidential Information, including information about Clients' Axes or trading activity. In the example above, the asset manager discloses and solicits Confidential Information, in this case another bank's Axe. In the example below, the asset manager refrains from soliciting Confidential Information.

✓ Market Participant ABC to Asset manager: We have an Axe in BTC. Do you have any interest? Asset manager to bank market maker: Thanks for calling but we don't have interest in BTC today.

X Hedge fund to bank market maker: Are you long BTC?

Market Participants should not solicit Confidential Information, including information on current positioning or trading activity, without a valid reason to do so. In the acceptable example below, the hedge fund asks for market views and not specific positioning.

✓ Hedge fund to bank market maker: What do you think of BTC here?

X A Market Participant has been asked by a Client to provide a quote for 300 BCH. The Market Participant does not actively market make in this currency pair. The Market Participant calls another market maker: I'm being asked to quote a two-way price for 300 BCH. Can you show me your BCH pricing matrix so that I can get a feel for the spread to quote?

Market Participants should not disclose or solicit Confidential Information, including information about Clients' trading activity. In the example above, the Market Participant discloses and solicits Confidential Information—in this case, the Client interest and the proprietary spread matrix information, respectively. In the example below, the OTC Desk requests only information pertinent to their needs.

✓ An OTC Desk has been asked by a Client to provide a quote for 10,000 BCH. The OTC Desk does not have a franchise in BCH, so their market maker calls another OTC Desk: Can you give me a two-way price for 10,000 BCH?

- **X** A Market Participant has implemented an institution-wide policy designating trade recommendations produced by the Cryptoasset Research Department as confidential until published to all Clients simultaneously. Market Participant Cryptoasset research analyst to hedge fund: Our view on BTC has shifted in line with our new central bank rate forecasts and I'm publishing a new bullish trade recommendation later today.

Market Participants should not disclose Confidential Information. In this example, the analyst has disclosed Designated Confidential Information—its trade recommendation—to an external party prior to publication. In the example below, the Cryptoasset research analyst discloses research after it has been published.

- ✓ Cryptoasset research analyst to hedge fund: I'm calling to check that you've received our bullish BTC trade recommendation published an hour ago in line with our new central bank rate forecasts.

- **X** A hedge fund manager attends a portfolio review with a large Client. At the review, the manager learns that the Client will soon be shifting part of its allocation into another Cryptoasset. The manager is asked for advice, but not awarded the allocation mandate. Upon leaving the meeting, the manager makes a call to his own trading desk to inform them of the impending trade.

Market Participants should not disclose Confidential Information except to those individuals who have a valid reason to receive such information. In particular, information obtained from a Client is to be used only for the specific purpose for which it was given. In this example, planned Cryptoasset reallocation is Confidential Information and has been disclosed to the hedge fund manager for advice only. It should not be disclosed to the trading desk.

- **X** A fund asks a Market Participant to work a large buy order of BTC. Immediately after the call, the bank contacts a different Client hedge fund and says, "I have a large buy order of BTC for a Client. I think this may move the market upwards in the next 20 minutes, and I can work some flow for you as well."

Past, present, and future Client trading activity is Confidential Information that should not be disclosed to other Market Participants.

<u>Market Participants should communicate in a manner that is clear, accurate, professional, and not misleading. (Principle 23)</u>

- **X** An asset manager calls three OTC Desks and says, "Can I get a price in 100 BTC, please? This is my full amount." The asset manager buys 100 BTC from each of the three banks for a total of 300 BTC.

Market Participants should communicate in a manner that is clear, accurate, professional, and not misleading. In this example, the asset manager deliberately misleads the OTC Desks in order to potentially secure better pricing. If asked, the asset manager could decline to disclose whether its request to transact is for the full amount.

- **X** A sell-side institution has a large amount of an illiquid Cryptoasset to sell. A trader at the institution contacts several Market Participants, saying that he is hearing of a very large buyer in this Cryptoasset, when this is in fact not the case.

Market Participants should communicate in a manner that is not misleading. In this example, the trader communicates false information with the intent of moving the market in his own interests.

Market Participants should communicate Market Color appropriately. (Principle 24)

- ✓ A corporate Client has left a 24-hour call level for BCH with a counterparty and the call level has just been breached. OTC Desk salesperson to corporate Client: BCH just traded through your call level. The market has dropped 20% in the last 15 minutes, there has been large selling across a variety of names, and prices have been gapping. The market continues to be better offered, but the move seems to be limited to just BCH. We don't know the trigger but there has been some chatter on the Internet about a 51% attack, but it has not been confirmed on any of the main news sources.

Market Participants should communicate Market Color appropriately and without compromising Confidential Information. In this example, the salesperson shares information about recent market developments, with the flow having been sufficiently aggregated and the information from a third party attributed clearly (Principle 23).

- ✓ A firm operating an anonymous multi-dealer Cryptoasset-Trading Venue asks users (as part of standard on boarding and/or "Know Your Client" information gathering) if they are signatories to the current version of the Global Cryptoasset Standards Statement of Commitment. This information is uploaded into a database in the same way that other user information is stored. This information could be included along with other tag information the platform provides, if applicable, or could be added to standard post-trade analytical reports.

Anonymous Trading Venues should strive to make available to users whether a counterparty or potential counterparty to a trade has represented that it has signed a Statement of Commitment to the current version of the Global Cryptoasset Standards. In this example, the firm uses its onboarding process to record the Statement of Commitment signatory status of its users.

- **X** Market Participant salesperson to hedge fund: We've seen large BTC demand from XYZ (where "XYZ" is a code name for a specific Client) this morning.

Market Participants should communicate Market Color appropriately, sharing flow information on an anonymized and aggregated basis only. In the example above, the information reveals the identity of a specific Client. In the example below, the communication is aggregated in terms of Client category so that the Client cannot be identified.

- ✓ OTC Desk salesperson to hedge fund: We've seen large BTC demand from Real Money names this morning.
- **X** Asset manager to an OTC Desk: I hear that you've been a big buyer of BTC. Is it for the same UK corporate(s) again?

Market Participants should not solicit Confidential Information, including the trading activity of a specific Client. Market Color should be anonymized and aggregated so as not reveal the flows related to a specific Client. In the example above, the asset manager has solicited Confidential Information. In the example below, the asset manager has solicited general Market Color.

- ✓ Asset manager to market maker: Can you give me some color around the price rally in BTC in the past hour?
- **X** Market maker to hedge fund: BCH liquidity has deteriorated. Just now it took me 15 ticks to cover my sale of 8,000 BCH to our biggest liquidity provider.

Market Participants should communicate Market Color appropriately, sharing flow information on an anonymized and aggregated basis only. In the example above, the communication refers to a specific recent trade and possibly reveals the identity of a specific Client. In the acceptable example below, the reference to the timing of execution is broad and the type of Client is generalized.

- ✓ Market maker to hedge fund: BTC liquidity has deteriorated. Last week I was able to trade 8,000 BCH for only 3 ticks, but today it took 15 ticks and twice as long.

Market Participants should have clear guidance on approved modes and channels of communication. (Principle 25)

- **X** A sales person has a number of filled orders to confirm to the customer but has left the office early. Not having access to a recorded line, he subsequently texts his confirmations from his own unrecorded personal cell phone to the Client.

It is recommended that communication channels be recorded, particularly when being used to transact. In the example above, the sales person confirms transactions on an unrecorded line. In the example below, the sales person strives to find a way to have the transactions confirmed via recorded means.

- ✓ A sales person has a number of filled orders to confirm to the customer but has left the office early. Not having access to a recorded line, the sales person contacts his office colleagues, who then contact the customer to confirm the transactions using recorded means.

RISK MANAGEMENT AND COMPLIANCE

Market Participants should have practices in place to limit, monitor, and control the risks related to their Cryptoasset Market trading activity. (Principle 29)

- **X** A Client of a Market Participant accesses Cryptoasset Market liquidity only through the Cryptoasset Trading Venue offered by the sales/trading business of the Market Participant and has no other source of liquidity. The Client has not evaluated the risks of relying on just one source of liquidity. In response to an unexpected market event, the Market Participant adjusts the liquidity provided through its Cryptoasset Trading Venue, which has the effect of severely impacting the ability of the Client to manage its Cryptoasset positions. As the Client has no

contingency in place to access the market (including relationship with the voice sales/trading business), the Client's ability to trade is compromised.

Market Participants should have practices in place to limit, monitor, and control the risks related to their Cryptoasset trading. In particular, Market Participants should be aware of the risks associated with reliance on a single source of liquidity and incorporate contingency plans as appropriate. In this example, the Client is unaware that its reliance on a single source of liquidity poses risks to its business and has no contingency plan in place, which severely limits its ability to manage its Cryptoasset positions.

✓ A Market Participant has a significant Client franchise and maintains several channels to access liquidity, including two Cryptoasset Prime Brokers and some bilateral agreements. For operational efficiency, the Market Participant routes the majority, but not all, of its flows through one of its Prime Brokers but has a smaller but representative part of its portfolio channeled regularly to the other Prime Broker and to its bilateral relationships.

Market Participants should be aware of the risks associated with reliance on a single source of liquidity and incorporate contingency plans as appropriate. In this example, the Market Participant has opted to maintain and use several liquidity sources as appropriate to the nature of its business.

X A small proprietary trading fund copies the risk checks that are those specified by its Prime Broker to stay within prudent limits, including Net Open Position (NOP) and Daily Settlement Limits (DSL). The fund's trading algorithm has a programming bug that causes a runaway algorithm that systematically loses money. The fund discovers that, despite their limit checks, the fund incurs losses that threaten the survival of the fund.

Market Participants should have practices in place to limit, monitor, and control the risks related to their Cryptoasset trading. In this example, the trading fund had inadequate processes in place to identify and manage operational risks specific to its business. The limit checks failed to alert the fund to a decline in position value. In the extreme, an algorithm that systematically loses, rather than earns, money can still be wholly within NOP and DSL limits because the position will fall in value.

<u>Market Participants should have Business Continuity Plans (BCPS). (Principle 35)</u>

X A Market Participant uses a backup site in the same region and relies on personnel in the same area as its primary site. The Market Participant has not developed a Business Continuity Plan appropriate to the nature, scale, and complexity of its business. During a civil emergency, the Market Participant finds that it is unable to access either the primary or the backup site because the two sites share the same telecommunications path. It also finds that it cannot reach personnel essential to its business.

Market Participants should have business continuity plans in place that are appropriate to the nature, scale, and complexity of their business and that can be implemented quickly and effectively. In this example, despite maintaining a primary and a backup site, the Market Participant did not have a business continuity plan that was robust to the disruption. In the two examples below, the Market Participant has made a business continuity plan that is, in each case, appropriate given the nature, scale, and complexity of its operations.

- ✓ A Market Participant selects a backup site that is geographically distant, and whose infrastructure can be controlled by personnel in the distant location.

- ✓ A Market Participant decides that it will not maintain a backup data center and, in the event that its data center is unavailable, will reduce or eliminate its positions by telephoning one of the market makers with whom it has a relationship and trade by voice only until its data center is available again.

Prime Brokerage Participants should strive to monitor and control trading permissions and credit provision in Real Time at all stages of transactions in a manner consistent with the profile of their activity in the market to reduce risk to all parties. (Principle 51)

- **X** A Prime Brokerage Client is provided with exposure limits for each of its executing dealers under its PB agreement. The Client assumes that the executing dealers are monitoring these limits and does not incorporate pre-trade compliance checking procedures within its internal processes. The PB Client trades on behalf of a number of underlying accounts in a bulk ticket, providing the executing Dealer with the PB account portion of the deal post-trade. The Client breaches its PB exposure limit with the executing dealers and is only made aware of the breach by the executing Dealer at the point of providing the breakdown.

Prime Brokerage Clients should strive to monitor their applicable limits as specified in their Prime Brokerage agreement. This is especially important where an executing Dealer is unaware of the precise account breakdown on a bulk transaction. Clients should have pre-trade compliance-monitoring procedures in place such that only trades that fit within the designation limits are requested of executing dealers.

- ✓ An executing broker notices a Client repeatedly breaching its authorized limits thanks to routine, embedded controls, and informs the Client, with a warning.

Prime Brokerage Participants should strive to monitor and control credit provision in Real Time. While this example notes a negative scenario (breaching of authorized limits), it is a positive example as the executing broker displays appropriate monitoring of risk controls to detect repeated limit breaches and appropriate information sharing among the affected parties.

CONFIRMATION AND SETTLEMENT

Market Participants should confirm trades as soon as practicable, and in a secure and efficient manner. (Principle 56)

- ✓ A Client executes a transaction in spot USD/BTC on a single-exchange platform and is immediately provided with a trade confirmation via the exchange's platform. After having checked the trade details received from the exchange, the Client is able to immediately send a confirmation message for the trade to the exchange.

Market Participants should confirm trades as soon as possible, and in a secure and efficient manner. In this example, the bank's straight-through-processing and initiation of the confirmation process results in the Client being able to send a corresponding confirmation message within a short time frame.

- ✓ A local Market Participant executes an Cryptoasset transaction with its parent entity via phone. Both the local entity and its parent confirm the deal directly via a common secured electronic platform.

Market Participants should confirm trades as soon as possible, and in a secure and efficient manner. In this example, both entities use a common secured electronic platform to confirm the deal—an alternative to market wide automated trade confirmation matching systems.

Market Participants should review, affirm, and allocate block transactions as soon as practicable. (Principle 57)

- **X** A corporate treasurer has a busy morning in meetings. There are ten trades to do, including some block trades with sub-allocations for the pension fund. The treasurer calls a counterparty by phone, completes all ten trades with just enough credit, and waits to input all of the trades into the system until after lunch.

Block transaction details should be reviewed and affirmed as soon as practicable following execution. In this example, the time lag between execution and input does not comply with this principle and can lead to delays in confirming.

ANNEX 2:

Glossary of Terms

Agent: A Market Participant that executes orders on behalf of its Clients pursuant to the Client mandate, and without taking on market risk in connection with the order.

Algorithmic Execution: Trade execution through computer programs that apply algorithms. For example, at the most basic level, a computer program automates the process of splitting a larger order known as the 'parent order' into multiple smaller orders known as 'child orders', and executes them over a period of time.

Applicable Law: With respect to a Market Participant, the laws, rules, and regulations applicable to it and the Cryptoasset Market in each jurisdiction in which it does business.

Axe: An interest that a Market Participant might have to transact in a given product or currency pair at a price that may be better than the prevailing market rate.

Client: A Market Participant requesting transactions and activity from, or via, other Market Participants that provide market making or other trade execution services in the Cryptoasset Market. A Market Participant can act as a Client in some instances while making markets in other instances.

Compliance Risk: Risk of legal or regulatory sanctions, material financial loss, or loss to reputation as a result of a Market Participant's failure to comply with laws, regulations, rules, industry standards, and

codes of conduct applicable to its Cryptoasset activities. Compliance concerns include observing proper standards of market conduct, managing conflict of interest, treating customers fairly, and taking measures for the prevention of money laundering and terrorist financing.

Confidential Information: Information that is to be treated as confidential, including Cryptoasset Trading Information and Designated Confidential Information.

Cryptoasset: Cryptographically secured digital representations of value or contractual rights that use public blockchains and can be transferred, stored, or traded electronically.

Cryptoasset Trading Venue: Any system that allows Market Participants to execute trades or input orders in a limit order book.

Cryptoasset Market: The wholesale Cryptoasset market.

Cryptoasset Trading Information: Can take various forms, including information relating to the past, present, and future trading activity or positions of the Market Participant itself or its Clients, as well as related information that is sensitive and is received in the course of such activity.

Designated Confidential Information: Confidential, proprietary, and other information for which Market Participants may agree to a higher standard of non-disclosure, which, at their discretion, may be formalized in a written non-disclosure or similar confidentiality agreement.

Direct Payment: The transfer of funds in settlement of a Cryptoasset transaction to the account of the counterparty to the transaction.

Electronic Trading Activities: These activities may include operating a Cryptoasset Trading Venue, making and/or taking prices on a Cryptoasset Trading Venue, and providing and/or using trading algorithms on an Cryptoasset Trading Venue.

Fixing Order: An order to transact at a particular fixing rate.

Give-Up: A process by which trades are passed on to a Prime Broker by a party designated by the Prime Broker to execute transactions with a Prime Broker Client.

Global Cryptoasset Standards: A set of global principles of good practices in the Cryptoasset Market.

Issuer: Issuer refers to a party that issues tokens and covers a number of entities including developers, designers, firms who issue tokens, and certain intermediaries since determining precisely who the issuers are is not always easy or possible.

Legal Entity Identifier (LEI): The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO).

Over-the-counter Desk (OTC Desk): A function provided by some Market Participants, where buyers and sellers are matched to execute bespoke transactions that may not be available or possible to execute in an automated fashion on automated exchanges.

Mark Up: The spread or charge that may be included in the final price of a transaction in order to compensate the Market Participant for a number of considerations, which might include risks taken, costs incurred, and services rendered to a particular Client.

Market Color: A view shared by Market Participants on the general state of, and trends in, the market.

Market Order: A request or communication from a counterparty to enter into a Cryptoasset transaction with a Market Participant for the sale or purchase of an Cryptoasset at the current available level.

Market Participant: See the detailed definition provided in the Foreword.

Personal Dealing: Where personnel deal for their personal account or indirect benefit (for example, for their immediate family members or other close parties).

Pre-Hedging: The management of the risk associated with one or more anticipated Client orders, designed to benefit the Client in connection with such orders and any resulting transactions.

Prime Broker (PB): An entity that provides credit intermediation to one or more parties to a trade based on pre-agreed terms and conditions governing the provision of such credit. The Prime Broker can also offer subsidiary or allied offerings, including operational and technology services.

Prime Brokerage Participant: A Market Participant that is either (i) a Prime Broker, (ii) a Client using the services of a Prime Broker, or (iii) a Market Participant acting as an executing dealer (price maker) or execution intermediary (such as an Agent or platform) between the Prime Brokerage Client and the Prime Broker.

Principal: A Market Participant who transacts for its own account.

Real Time: Near, or close to, the actual time during which a process or event occurs.

Settlement Risk: The risk of outright loss of the full value of a transaction resulting from the counterparty's failure to settle. This can arise from paying away the currency being sold, but failing to receive the currency being bought. (Settlement Risk is also referred to as "Herstatt Risk.")

SSI: Standing settlement instruction.

Standards: The Global Cryptoasset Standards contained within this document.

Stop Loss Orders: A contingent order that triggers a buy or sell order for a specified notional amount when a reference price has reached or passed a pre-defined trigger level. There are different variants of Stop Loss Orders, depending on the execution relationship between counterparties, the reference price, the trigger, and the nature of the triggered order. A series of parameters are required to fully define a Stop Loss Order, including the reference price, order amount, time period, and trigger.

Third-Party Payment: The transfer of funds in settlement of a Cryptoasset transaction to the account of an entity other than that of the counterparty to the transaction.

Voice Broker: A Broker with responsibility to both counterparties, who negotiates Cryptoasset transactions via telephone, conversational systems, and/or hybrid solutions.

ANNEX 3:

Statement of Commitment

STATEMENT OF COMMITMENT TO THE GLOBAL CRYPTOASSET STANDARDS

[Name of institution] has reviewed the content of the Global Cryptoasset Standards ("Standards") and acknowledges that the Standards represent a set of principles generally recognized as good practice in the wholesale Cryptoasset Market. The Institution confirms that it acts as a Market Participant as defined by the Standards, and is committed to conducting its Cryptoasset Market activities ("Activities") in a manner consistent with the principles of the Code. To this end, the Institution has taken appropriate steps, based on the size and complexity of its Activities, and the nature of its engagement in the Cryptoasset Market, to align its Activities with the principles of the Standards.

[Name of institution]

Date: _____

Explanatory Note to the Statement of Commitment to the Global Cryptoasset Standards

The Global Cryptoasset Standards ("Standards") set out globally recognized principles of good practice in the wholesale Cryptoasset market ("Cryptoasset Market"). It is designed to promote a robust, fair, liquid, open, and appropriately transparent market, to help build and maintain market confidence, and in turn, to improve market functioning. The Statement of Commitment ("Statement") provides Market Participants with a common basis by which they can demonstrate their recognition of, and commitment to, adopting the good practices set forth in the Standards.

1. How should the Statement be used and what are the benefits?

The Statement has been developed to support the objectives of the Standards such as enhancing transparency, efficiency, and functioning in the Cryptoasset Market. To that end, it provides a means by which (i) Market Participants can signal their intention to adopt, and adherence to, the Standards' good practices, and (ii) Market Participants, and others, can more objectively assess the operational and compliance infrastructures of other Market Participants. Like the Standards, the Statement is voluntary, and Market Participants may choose to make use of it in different ways. For example, Market Participants may use the Statement publicly, by publishing it on their website, or bilaterally, by providing it directly to other Market Participants, such as existing or prospective Clients or counterparties.

Among the primary benefits of using the Statement is raising awareness of the Standards and promoting its objectives in a pro-competitive manner. Use and publication of the Statement provides a positive signal to Clients, counterparties, and the wider market, of a Market Participant's commitment to following good practice. Widespread use of the Statement will raise the profile of the Standards, supporting a common understanding across the Cryptoasset Market of what constitutes good practice in key areas and encouraging the broadest constituency of Market Participants to engage with and support the Standards and its objectives.

2. What does using the Statement represent?

It represents that a Market Participant:

(i) has made an independent determination to support the Standards and recognizes it as a set of principles of good practice for the Cryptoasset Market;

(ii) is committed to conducting its Cryptoasset Market activities in a manner that is consistent with the principles of the Standards; and

(iii) considers that it has taken appropriate steps, based on the size and complexity of its activities, and the nature of its engagement in the Cryptoasset Market, to align its activities with the principles of the Standards.

Whether and to what extent a Market Participant adopts and implements the guidelines set forth in the Standards is a decision that each Market Participant should make for itself, as is the decision of whether and to what extent a Market Participant elects to utilize the Statement of Commitment.

3. Market Participants vary, for instance, in relation to the size and nature of their Cryptoasset Market activities. How is that taken into account?

As noted in the Foreword to the Standards, the Cryptoasset Market features a diverse set of participants who engage in the Cryptoasset Market in different ways and across various Cryptoasset products. Both the Standards and the Statement have been written and should be interpreted with this diversity in mind.

What this means in practice is that the steps each Market Participant takes to align its activities with the principles of the Standards will reflect the size and complexity of its Cryptoasset Market activities, and the nature of its engagement in the Cryptoasset Market, and will take account of Applicable Law. Ultimately, the decision of what steps should be undertaken in support of a Market Participant's Statement, and in what manner, resides with each Market Participant, reflecting an appropriate internal assessment. For some Market Participants, appropriate steps may include reviewing their practices in light of the Standards and establishing and maintaining policies, procedures, and controls reasonably designed to support their commitment. In addition, Market Participants might assess the appropriate levels of senior management oversight and establish dedicated staff training or embed into existing training.

4. How should Market Participants take account of their corporate structure?

This is a matter for each Market Participant to determine. The Statement has been designed flexibly to accommodate group companies providing a single, group-level statement, or individual group entities providing their own statements.

5. What processes should a Market Participant consider implementing before using the Statement?

Market Participants should consider what type of governance and approval processes would be appropriate for them to implement in connection with their use of the Statement. These processes will vary between Market Participants, but it is anticipated that the individual, or group of individuals, responsible for approving the Market Participant's use and publication of the Statement will have appropriate oversight of the Market Participant's Cryptoasset Market activities and the authority to make statements of the type contained in the Statement. A Market Participant's assessment of the appropriateness of its own implementation policies and practices should be made independently from the assessment by other Market Participants.

6. When should a Market Participant start using the Statement?

As noted above, Market Participants may take different steps to support their use of the Statement. The time taken to implement such steps may vary depending on the current practices of the Market Participant and the size and nature of the Market Participant's business. Having considered feedback from a broad range of Market Participants, it is anticipated that most Market Participants will need approximately 6 to 12 months to prepare to use the Statement.

7. How frequently should a Market Participant review/renew their Statement?

Given that the nature of a Market Participant's business may change over time, Market Participants that use the Statement should consider what steps they will take to review their activities for alignment with the Standards' principles. The steps taken should reflect the size and complexity of the Market Participant's Cryptoasset Market activities and the nature of its engagement in the Cryptoasset Market. Whereas some Market Participants may consider setting a regular schedule for review, others may vary their approach based on how their business changes over time.

In addition, it is anticipated that the Standards will be updated from time to time to reflect emerging issues, changes in the Cryptoasset Market, and feedback from Market Participants and others. Upon publication of future updates to the Standards, Market Participants should consider renewing their Statement, having regard to the nature of those updates, as well as the size and complexity of their Cryptoasset Market activities and the nature of their engagement in the Cryptoasset Market.