



**Canadian Securities
Administrators**

**Autorités canadiennes
en valeurs mobilières**

**Joint Canadian Securities Administrators/Investment Industry
Regulatory Organization of Canada**

Consultation Paper 21-402

Proposed Framework for Crypto-Asset Trading Platforms

March 14, 2019

PART 1 – Introduction and purpose

The emergence of “digital assets” or “crypto assets” continues to be a growing area of interest for regulators globally. Innovations like distributed ledger technology (**DLT**) and crypto assets are relatively new and are transforming the landscape of the financial industry. Interest in crypto assets among investors, governments and regulators globally has increased significantly since the creation of bitcoin in 2008 and continues to grow. Early in 2018, at its peak, the total value of crypto assets was estimated, by one source, at more than US\$800 billion.¹ While the value has since fallen, trading volumes remain significant. Today, there are over 2000 crypto assets² that may be traded for government-issued currencies or other types of crypto assets on over 200 platforms³ that facilitate the buying and selling or transferring of crypto assets (**Platforms**). Many of these Platforms operate globally and without any regulatory oversight.

Although DLT may provide benefits, global incidents point to crypto assets having heightened risks related to loss and theft as compared to other assets. Regulators around the world are currently considering important issues surrounding the regulation of crypto assets including the appropriate regulation of Platforms. The Canadian Securities Administrators (the **CSA**) and the Investment Industry Regulatory Organization of Canada (**IIROC**, and together with the CSA, **we**), have been engaged with regulators globally, through IOSCO and other innovation initiatives, to seek input on a variety of regulatory approaches that exist in this area.

Platforms, depending on how they operate and the crypto assets they make available for trading may be subject to securities regulation. The CSA, through its Regulatory Sandbox⁴, is in discussions with several Platforms that are seeking guidance on the requirements that apply to them. We have heard directly from Platform operators and their advisers that a regulatory framework is welcome, as they seek to build consumer confidence and expand their businesses across Canada and globally.

Currently there are no Platforms recognized as an exchange or otherwise authorized to operate as a marketplace or dealer in Canada. As such, the CSA has urged Canadians to be cautious when buying crypto assets.⁵

Platforms facilitate the buying and selling of crypto assets and perform functions similar to one or more of exchanges, alternative trading systems (**ATSs**), clearing agencies, custodians and dealers. Depending on their structure, they may also introduce novel features which create risks to investors and our capital markets that may not be fully addressed by the existing regulatory framework. Where securities legislation applies to Platforms we are considering a set of tailored regulatory requirements for them to address the novel features and risks (the **Proposed Platform Framework**).

¹ <https://coinmarketcap.com/charts/>.

² Coinmarketcap.com listed 2098 different crypto assets as of March 1, 2019. See: <https://coinmarketcap.com/all/views/all/>.

³ Coinmarketcap.com listed 241 Platforms as of March 1, 2019. See: <https://coinmarketcap.com/rankings/exchanges/3>.

⁴ The CSA Regulatory Sandbox is an initiative of the CSA to support businesses seeking to offer innovative products, services and applications in Canada.

⁵ The CSA has previously issued investor alerts reminding investors of the [inherent risks associated with crypto asset futures contracts](#) and [the need for caution when investing with crypto asset trading platforms](#).

We endeavor to facilitate innovation that benefits investors and our capital markets, while ensuring that we have the appropriate tools and understanding to keep pace with evolving markets. The purpose of this joint CSA/IIROC Consultation Paper (the **Consultation Paper**) is to seek feedback from the financial technology (**fintech**) community, market participants, investors and other stakeholders on how requirements may be tailored for Platforms operating in Canada whose operations engage securities law. We intend to use this feedback to establish a framework that provides regulatory clarity to Platforms, addresses risks to investors and creates greater market integrity.

Throughout the Consultation Paper, investors participating on Platforms may be referred to as either **investors** or **participants**.

PART 2 – Nature of crypto assets and application of securities legislation⁶

Crypto assets differ in their functions, structures, governance and rights. Some crypto assets, commonly referred to as “utility tokens”, are created to allow holders to access or purchase goods or services on a DLT network being developed by the creators of the token. As set out in [CSA Staff Notice 46-307 *Cryptocurrency Offerings*](#) and [CSA Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens*](#), staff of the CSA have found that most of the offerings of utility tokens have involved a distribution of securities, usually as investment contracts. Other crypto assets are tokenized forms of traditional securities or derivatives and may represent an interest in assets or have their value may be based on an underlying interest. If crypto assets that are securities and/or derivatives are traded on a Platform, the Platform would be subject to securities and/or derivatives regulatory requirements.

We note that it is widely accepted that at least some of the well established crypto assets that function as a form of payment or means of exchange on a decentralized network, such as bitcoin, are not currently in and of themselves, securities or derivatives. Instead, they have certain features that are analogous to existing commodities such as currencies and precious metals.

However, securities legislation may still apply to Platforms that offer trading of crypto assets that are commodities, because the investor’s contractual right to the crypto asset may constitute a security or derivative. We are evaluating the specific facts and circumstances of how trading occurs on Platforms to assess whether or not a security or derivative may be involved. Some of the factors we are currently considering in this evaluation include:

- whether the Platform is structured so that there is intended to be and is delivery of crypto assets to investors,
- if there is delivery, when that occurs, and whether it is to an investor’s wallet over which the Platform does not have control or custody,
- whether investors’ crypto assets are pooled together with those of other investors and with the assets of the Platform,
- whether the Platform or a related party holds or controls the investors’ assets,

⁶ As defined in National Instrument 14-101 *Definitions*.

- if the Platform holds or stores assets for its participants, how the Platform makes use of those assets,
- whether the investor can trade, or rollover positions held by the Platform, and
- having regard to the legal arrangements between the Platform and its participants, the actual functions of the Platform and the manner in which transactions occur on it
 - who has control or custody of crypto assets,
 - who the legal owner of such crypto assets is, and
 - what rights investors will have in the event of the Platform's insolvency.

Consultation question

1. Are there factors in addition to those noted above that we should consider?

The CSA wishes to remind market participants that any person or company advertising, offering, selling or otherwise trading or matching trades in crypto assets that are securities or derivatives, or derivatives that are based on crypto assets to persons or companies in Canada, or conducting such activities from a place of business in Canada is subject to securities legislation in Canada. Further, as noted above, although some crypto assets may be commodities, securities legislation may still apply to Platforms that offer trading of such crypto assets because the investor's contractual right to the crypto asset/commodity may constitute a security or derivative. Further, in most jurisdictions in Canada, the provisions of securities legislation relating to fraud, market manipulation and misleading statements apply not just to the trading of securities and derivatives but also to trading of the underlying interest of a derivative (e.g. the commodity).

The Proposed Platform Framework referred to in this Consultation Paper considers how existing regulatory requirements may be tailored for Platforms and should not be construed as acceptance by the CSA that securities and/or derivatives legislation may not apply to any particular offering involving crypto assets.

PART 3 – Risks related to Platforms

The operational models and the risks related to Platforms may vary from one platform to another; however, the risks are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers. The introduction of crypto assets and the operational models of Platforms, however, raise different and in some cases heightened, areas of risk. Key areas of risk include:

- **Investors' crypto assets may not be adequately safeguarded** – Many Platforms have control of their participants' crypto assets (e.g. they keep participants' crypto assets in a single account on the distributed ledger under the Platform's private key or the Platform holds its participants' private keys on their behalf). Platforms may not have necessary processes and controls in place to segregate participants' assets from their own and to safeguard those assets, including maintaining and safeguarding any private keys associated with wallets held by the Platform. There are also current challenges associated with auditing the internal controls surrounding custody of participants' assets.

- **Processes, policies and procedures may be inadequate** – Platforms may not have sufficient processes, policies and procedures in place to establish an internal system of controls and supervision sufficient to prudently manage the risks associated with their business, including business continuity risks, key personnel risks and regulatory compliance risks.
- **Investors’ assets may be at risk in the event of a Platform’s bankruptcy or insolvency** – Platforms may not segregate participants’ assets from their own or may use participants’ assets to fund operating costs and other expenses. As a result, Platforms may not hold sufficient assets to cover investor claims and return investors’ assets in the event of bankruptcy or insolvency. In addition, Platforms may operate in jurisdictions that have limited asset protection and insolvency regimes.
- **Investors may not have important information about the crypto assets that are available for trading on the Platform** – Each crypto asset has its own functions, associated rights and risks. Platforms may not provide sufficient or clear information about the crypto assets for participants to make informed investment decisions. Examples of information may include the standards that the crypto asset had to meet before being admitted for trading on the Platform and any potential difficulties in liquidating the crypto asset.
- **Investors may not have important information about the Platform’s operations** – Platforms may not provide sufficient information about the functions they perform and their fees. For example, some Platforms do not deliver crypto assets to a wallet controlled by the participant unless requested, but participants may not be aware of this or the risks associated with the Platform retaining custody of their crypto assets, including that they may not be able to access their crypto assets.
- **Investors may purchase products that are not suitable for them** – Exchanges and other regulated marketplaces do not interact directly with retail investors; instead they interact through regulated intermediaries (i.e. registered dealers). In contrast, Platforms may offer investors (including retail investors) direct access to the Platform without the use of a regulated intermediary that performs know-your-client and suitability assessments. As a result, participants may purchase crypto assets, many of which can be complex, high risk and volatile products, that are not suitable investments for them.
- **Conflicts of interest may not be appropriately managed** – There may be conflicts of interest between the Platform’s operator and participants who access the Platform, including the inherent conflicts of interest where Platforms act as market makers and trade as principal.
- **Manipulative and deceptive trading may occur** – Platforms may be susceptible to manipulative and deceptive trading given the market volatility, lack of reliable pricing information for crypto assets, the fact that they trade 24 hours daily and the fact that trading on many Platforms is not currently monitored.
- **There may not be transparency of order and trade information** – Information relating to the price and volume of orders and trades may not be publicly available or sufficient to support efficient price discovery.
- **System resiliency, integrity and security controls may be inadequate** – Platforms have significant cybersecurity risks. DLT is a nascent technology and Platform operators may not have sufficient experience or possess the necessary skills to ensure that systems function properly and there is adequate protection against cyber theft of participants’ crypto asset investments.

Consultation question

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

PART 4 – Regulatory approaches in other jurisdictions

In developing the Proposed Platform Framework, we considered the approaches taken by securities and financial regulators in other jurisdictions. We found that in many jurisdictions the existing regulatory requirements will apply to regulate Platforms within those jurisdictions. Some jurisdictions may tailor requirements or provide exemptions. This means that the regulatory requirements applicable to exchanges, ATs (in the U.S. or Canada), multilateral trading venues (in Europe) and other regulated markets may apply to a Platform.

In the U.S., the Securities and Exchange Commission (**SEC**) issued a statement indicating that, if a platform offers trading of digital securities and operates a marketplace, it must be registered with the SEC as a national securities exchange, registered with the Financial Industry Regulatory Authority as a broker-dealer operating an ATS, or be exempt from registration.⁷ The Commodity Futures Trading Commission (**CFTC**) has indicated that bitcoin and certain other crypto assets are encompassed in the definition of “commodity”. In the context of retail commodity transactions in crypto assets, for example on Platforms, the CFTC has consulted with market participants on its approach to the proposed interpretation of the term “actual delivery”.⁸

In European jurisdictions, the regulatory framework under the Markets in Financial Instruments Directive (**MiFID**) applies when crypto assets qualify as financial instruments. The European Securities and Markets Authority (**ESMA**) recently published a report with their advice on initial coin offerings and crypto assets where they identify the risks in the crypto asset sector.⁹ In the report, ESMA indicates that where crypto assets qualify as transferable securities or other types of MiFID financial instruments, the existing regulatory framework will apply. ESMA also noted that the existing requirements may not address all the risks, and in some areas, the requirements may not be relevant in a DLT framework.

In Singapore, Platforms that trade crypto assets that are securities may be approved exchanges or be recognised market operators and, in both cases, are subject to regulation by the Monetary Authority of Singapore.¹⁰

⁷ SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets (March 7, 2018):

<https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>.

⁸ CFTC, Retail Commodity Transactions Involving Virtual Currency, Proposed Interpretation, 82 Fed. Reg. 60335 (December 20, 2017): <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2017-27421a.pdf>.

⁹ ESMA Advice – Initial Coin Offerings and Crypto-Assets (January 9, 2019):

https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

¹⁰ Monetary Authority of Singapore, A Guide to Digital Token Offerings (last updated November 30, 2018):

<http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov%202018.pdf>

In Hong Kong, Platforms that are trading products that are not within the remit of the Hong Kong Securities and Futures Commission (**HKSFC**) can apply to use HKSFC's Regulatory Sandbox, particularly if they will, in the future, seek to offer trading of products that are within the remit of the HKSFC. This will allow the HKSFC to engage in an exploratory stage where it observes the Platform's operations and considers the effectiveness of proposed regulatory requirements for Platforms and whether Platforms are appropriate to be regulated by the HKSFC. If the decision is made to license the Platform, additional restrictions may apply.¹¹

In Malaysia, the *Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019* came into force on January 15, 2019 and specifies that all digital currencies, tokens and crypto assets are classified as securities, placing them under the authority of the Securities Commission Malaysia.¹²

Many financial regulators are proactively conducting inquiries into the activities of Platforms to determine if they are carrying on activities that require them to comply with their requirements.

Consultation question

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

PART 5 – The Proposed Platform Framework

5.1 Overview of the Proposed Platform Framework

The Proposed Platform Framework will apply to Platforms that are subject to securities legislation and that may not fit within the existing regulatory framework. It will apply both to Platforms that operate in Canada and to those that have Canadian participants.¹³

In developing the Proposed Platform Framework, the CSA considered that some of the Platforms are hybrid in nature and may perform functions typically performed by one or more of the following types of market participants: ATSS¹⁴, exchanges¹⁵ (exchanges and ATSS are both types of marketplaces¹⁶), dealers, custodians and clearing agencies. Specifically:

¹¹ HKSFC Conceptual framework for the potential regulation of virtual asset trading platform operators (November 1, 2018): https://www.sfc.hk/web/EN/files/ER/PDF/App%20-%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf

¹² Securities Commission Malaysia media release (January 14, 2019): <https://www.sc.com.my/news/media-releases-and-announcements/sc-to-regulate-offering-and-trading-of-digital-assets>

¹³ The CSA may consider exemptive relief from the applicable requirements if the Platform is located outside of Canada and is regulated by a foreign regulator in a manner that is similar to domestic oversight.

¹⁴ ATS is defined in every jurisdiction other than Ontario in s. 1.1 of National Instrument 21-101 *Marketplace Operation* (NI 21-101), and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

¹⁵ An exchange is a marketplace that may, among other things, lists the securities of issuers; provides a guarantee of a two-sided market for a security on a continuous or reasonably continuous basis; sets requirements governing the conduct of marketplace participants; or disciplines marketplace participants. Securities legislation enables securities regulatory authorities to recognize exchanges or exempt an exchange from recognition.

¹⁶ Marketplace is defined in every jurisdiction other than Ontario in s. 1.1 on NI 21-101, and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

- like an exchange or ATS, they may be a market or facility where orders of multiple buyers and sellers are brought together and matched;
- like an exchange, they may facilitate the creation or “listing” of a crypto asset;
- like an ATS or exchange, they may decide which crypto assets will be eligible for trading;
- like an exchange, they may offer a guarantee of a two-sided market and conduct regulatory activities;
- like a dealer, they may perform know-your-client and suitability reviews to grant access to investors (retail and institutional) and they may trade as principal;
- like a dealer or a custodian, they may self-custody investor’s assets or otherwise have control over investors’ assets; and
- like a clearing agency, they may enable the clearing and settlement of trades.

Application of marketplace requirements

The Proposed Platform Framework is based on the existing regulatory framework applicable to marketplaces and incorporates relevant requirements for dealers facilitating trading or dealing in securities. It is tailored to take into account the functions that may be performed by each Platform. Specifically, a Platform that brings together orders of buyers and sellers of securities and uses non-discretionary methods for these orders to interact is a marketplace.

As a marketplace, a Platform will be subject to requirements that will address many of the risks outlined in Part 3 of the Consultation Paper, such as those set out in NI 21-101, National Instrument 23-101 *Trading Rules* (**NI 23-101**) and, together with NI 21-101, the **Marketplace Rules**) and National Instrument 23-103 *Electronic Trading and Direct Access to Marketplaces* (**NI 23-103**).

Application of dealer requirements

In addition to marketplace functions, the Platform may also perform dealer functions, for example, providing custody of crypto assets and permitting direct access to trading by retail investors. As a result, the Proposed Platform Framework will include requirements that address the risks relating to these additional functions. Many of these requirements already exist in regulatory frameworks applicable to dealers.

Some entities will not fall within the definition of a marketplace. For example, an entity that is trading crypto assets that are securities but always trades against its participants and does not facilitate trading between buyers and sellers may be regulated as a dealer only and therefore not be subject to the Marketplace Rules and the Proposed Platform Framework. For example, firms that are currently registered in the category of exempt market dealer and that are currently permitted under securities legislation to facilitate the sale of securities, including crypto assets, in reliance on available prospectus exemptions in National Instrument 45-106 *Prospectus Exemptions* can continue to offer this service as long as they do not fall within the definition of “marketplace”.

Registered firms introducing crypto asset products and/or services are required to report changes in their business activities to their principal regulator and the proposed activities may be subject to review to assess whether there is adequate investor protection.

Investment dealer registration and IIROC membership

Like the Marketplace Rules, the Proposed Platform Framework contemplates Platforms both becoming registered as investment dealers and becoming IIROC dealer and marketplace members (**IIROC Members**)¹⁷. IIROC currently oversees all investment dealers as well as trading activity on debt and equity marketplaces in Canada and, accordingly,

- has a comprehensive body of rules governing the business, financial and trading conduct of IIROC Members which are tailored to the different types of products and services offered by IIROC Members;
- has established programs to assess compliance with both IIROC's rules applicable to dealers (**IIROC Dealer Member Rules**) and the Universal Market Integrity Rules (**UMIR**) that govern trading on a marketplace;
- has experience with dealers and marketplaces that trade a variety of securities and has developed tailored compliance programs and applied tailored rules for marketplaces; and
- operates in a regulatory capacity in every province in Canada.

Recognition as an exchange

A Platform that intends to carry on business as an exchange should contact the relevant securities regulatory authority to discuss whether recognition as an exchange is appropriate or, if such Platforms offer direct retail access or trade as principal, the Proposed Platform Framework is more appropriate to address risks arising from these activities.

Derivatives requirements

The CSA plans to consult on the appropriate regulatory framework to apply to marketplaces that trade over-the-counter derivatives, including platforms that offer derivatives with exposure to a crypto asset (e.g. a derivatives trading facility or swap execution facility that facilitate transactions in bitcoin-based derivatives). In the interim, if a Platform is trading or dealing in crypto assets that may be classified as derivatives, to the extent that the Platform has similar functions or operations to those contemplated in this Consultation Paper, it may be appropriate to apply requirements to those Platforms that are similar to the requirements contemplated by the Proposed Platform Framework. We anticipate, however, that such requirements may need to be specifically tailored to reflect the requirements that currently apply to derivatives or are otherwise appropriate to apply to those products and marketplaces.¹⁸

¹⁷ We note that IIROC membership may not be appropriate in all cases, depending on the facts and circumstances.

¹⁸ We would also like to remind market participants of the requirements relating to commodity futures exchange contracts in securities and commodity futures legislation.

5.2 Proposed Platform Framework - Key areas for consultation

While the Proposed Platform Framework builds on an existing regulatory regime that was designed for a wide variety of market participants, we recognize that the existing regulatory requirements, and particularly the Marketplace Rules, were designed for marketplaces trading traditional securities (such as equities and debt). The CSA supports innovation in our capital markets while protecting investors and promoting fair and efficient capital markets. We are therefore considering a set of requirements tailored to Platforms' operations that appropriately addresses the new risks introduced.

Below, we seek feedback on a number of areas that will assist in determining appropriate requirements for Platforms.

5.2.1 Custody and verification of assets

It has been reported that crypto assets with a value of almost US\$1 billion were stolen in 2018 from Platforms that operate globally.¹⁹ The ownership of crypto assets is evidenced by private keys which are required to execute crypto asset transactions. As the loss or theft of a private key may result in the loss of assets, the safeguarding of private keys is especially critical.

The operational model of many Platforms involves the Platform having custody of its participants' assets including private keys or the Platform holding the crypto assets in its own wallet with the Platform's private key. As a result, appropriate custody controls are a necessary part of managing risks to investors. To the extent that the Platform holds or has control over investors' assets, a significant risk is that investors' assets are not sufficiently accounted for or protected by the Platform. As a result, the Platform might not have sufficient crypto assets or cash to satisfy demand or could be vulnerable to theft. This risk increases substantially if there is insufficient insurance to cover the full amount of the theft.

When looking at the operations of a Platform, we will assess whether a Platform's risk management policies and procedures are appropriate to manage and mitigate the custodial risks. Expectations will be guided by the operational model of the Platform. For example, if the trades on a Platform do not occur on the distributed ledger, and instead the Platform keeps track of changes in ownership on its own internal ledger, we will evaluate whether the Platform has a robust system of internal controls, including records, that ensures that a participant's crypto assets are accurately accounted for by the Platform and appropriately segregated from assets belonging to the Platform.

Traditional custodians that hold assets for clients typically engage an independent auditor to perform an audit of the custodian's internal controls and prepare an assurance report. There are different types of assurance reports; however, it is common for custodians to engage external auditors to issue system and organization controls reports such as SOC 1 Reports²⁰ and SOC 2 Reports²¹ regarding the suitability of internal controls in financial reporting and controls

¹⁹ <https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2>.

²⁰ Report on controls at a service organization relevant to participant entities' internal control over financial reporting.

²¹ Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.

surrounding the custody of investors' assets. The auditor will issue a report pertaining to the design of the controls (**Type I Report**), and a report assessing whether such controls are operating as intended over a defined period (**Type II Report**). We anticipate that these reports will play an important role in the authorization and oversight of the Platform, reporting of transactions, internal risk management and verification of the existence of investors' assets. We contemplate requiring that Platforms obtain SOC 2, Type I and II Reports for their custody system and, if they use third-party custodians, to ensure that they have SOC 2, Type I and II Reports.

We understand, however, that there have been challenges with crypto asset custodians and Platforms obtaining SOC 2, Type II Reports, in part due to the novel nature of crypto asset custody solutions and the limited period of time that Platforms have been in operation to allow for the testing of internal controls. Nevertheless, we contemplate that Platforms seeking registration as an investment dealer registration and IROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined standards specific to the custody of crypto assets.

Consultation questions

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

5.2.2 Price determination

Fair and efficient capital markets are dependent on price discovery. The wide availability of information on orders and/or trades is important to foster efficient price discovery and investor confidence. As with traditional marketplaces, Platforms will be required to foster price discovery for the crypto assets they offer for trading. It is important for regulators and for the participants on the Platform to understand how prices on a Platform are determined. In addition, where the Platform or an affiliate acts as a market maker and provides quotes, the mechanisms for determining those quotes are expected to be available to participants. When trading as a market maker against its participants, a Platform will also be required to provide participants with a fair price.

Consultation questions

7. What factors should be considered in determining a fair price for crypto assets?

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

5.2.3 Surveillance of trading activities

The existing types of marketplaces have different regulatory responsibilities. Exchanges are responsible for conducting market surveillance of trading activities on the exchange and enforcing market integrity rules. All of the existing equity exchanges have retained IIROC to monitor trading activity and enforce market integrity rules. ATSS, by contrast, are not permitted to conduct market surveillance or enforcement activities and are required to engage a regulation services provider (**RSP**). IIROC currently acts as an RSP to all equity and fixed income marketplaces.

If IIROC were retained as an RSP by a Platform, IIROC would conduct market surveillance for that Platform. We understand that some of the types of manipulative and deceptive trading activities that may occur on Platforms that trade crypto assets are similar to those on marketplaces trading traditional securities. A unique challenge associated with market surveillance on Platforms is the fact that crypto assets trade on a global basis, on and off Platforms, outside regular trading hours, and may be illiquid and highly volatile. This, and the fact that there is currently no central source for pricing, may affect the price of a crypto asset trading on a Platform. This may also make it difficult to obtain reliable reference data that is needed to conduct effective surveillance.

To reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities, or extend margin to their participants. We may revisit this once we have a better understanding of the risks introduced to the market by the trading of crypto assets.

Some Platforms have indicated that they intend to set rules and monitor the trading activities of their marketplace participants rather than retaining an RSP. This may raise conflicts of interest issues that will need to be addressed.

Consultation questions

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

5.2.4 Systems and business continuity planning

System resiliency, reliability and security controls are important for investor protection. System failures may result in investors being unable to access their crypto assets and may have an impact on market efficiency and investor protection. Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber-attacks.²² Marketplaces are also required to maintain business continuity and disaster recovery plans to provide uninterrupted provision of key services.²³ To ensure that marketplaces have adequate internal and technology controls in place over their trading, surveillance and clearing systems and that their systems function as designed, marketplaces are required to engage an entity with relevant experience both in information technology and in the evaluation of related internal controls to conduct an independent systems review (**ISR**).²⁴

Technology and cyber security are key risks for Platforms. For these reasons they will also be required to comply with the systems and business continuity planning requirements applicable to existing marketplaces in NI 21-101. One key difference between Platforms and traditional marketplaces is that there is a greater risk for participants when a Platform provides custody of investors' crypto assets and does not have the appropriate internal controls.

In the normal course, all marketplaces are required to have an ISR conducted for other critical systems including order entry, execution or data. These requirements are in place to manage risks associated with the use of technology and to ensure that minimum standards are maintained. In some cases, we have granted temporary exemptions from the ISR requirements, provided the marketplace did not pose a significant risk to the capital markets and certain reports and information are provided to regulators.

Consultation question

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

5.2.5 Conflicts of interest

Platforms may have certain conflicts of interests, similar to other marketplaces. They may also raise a number of unique conflicts. For example, they may provide advice to their participants, which raises a conflict because the Platform may be providing advice on the same crypto assets that they have made eligible for trading on the Platform.

Another conflict relates to proprietary trading. Like dealers, it is possible that some Platforms trade for their own account against their participants, including retail investors. This raises conflicts of

²² Part 12 of NI 21-101.

²³ *Ibid.*

²⁴ *Ibid.*

interest and a number of risks, including that the Platform’s participants may not know that the Platform operator also trades on the marketplace against the investor and the risk that investors may not receive a fair price when trading against the Platform operator.

To address these risks, we contemplate that Platforms will be required to identify and manage potential conflicts of interest and will be required to disclose whether they trade against their participants, including acting as a market maker, and the associated conflicts of interest. Disclosure will assist investors in assessing whether they want to participate on the Platform. To the extent Platforms are required to become IIROC Members, they will also be subject to requirements in the UMIR aimed at mitigating the risks associated with trading against their participants.²⁵

Consultation questions

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

5.2.6 Insurance

Some Platforms have custody of investors’ assets. This makes them attractive targets for cyber-attacks and theft by insiders. Accordingly, insurance will also be an important safeguard. Dealers are required to maintain bonding or insurance against specific risks and in specified amounts.²⁶ This requirement may not address the specific operational risks of Platforms.

Many Platforms currently operate without any insurance covering investors’ assets. We note that there may be significant difficulty and costs for a Platform to obtain insurance, in part due to the limited number of crypto asset insurance providers, and the high risk of cyber-attacks. Therefore, some Platforms have indicated that they are considering limited coverage that only extends to certain crypto assets, crypto assets in “hot wallets” or “cold wallets”, loss as result of hacking, or loss from insider theft.

Consultation questions

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

²⁵ These include UMIR 5.3 *Client Priority*, UMIR 8.1 *Client Principal Trading* and UMIR 4.1 *Frontrunning*.

²⁶ s. 12.3 of NI 31-103.

5.2.7 Clearing and settlement

All trades executed on a marketplace are required to be reported and settled through a clearing agency.²⁷ A regulated clearing agency improves the efficiency of marketplaces and brings stability to the financial system.

Without exemptive relief, this requirement would also apply to Platforms that are marketplaces. However, currently there are no regulated clearing agencies for crypto assets that are securities or derivatives. As indicated above, we understand that on some Platforms, transaction settlement occurs on the Platform's internal ledger and is not recorded on the distributed ledger. We are considering whether an exemption from the requirement to report and settle trades through a clearing agency is appropriate. In these circumstances, Platforms will still be subject to certain requirements applicable to clearing agencies and will therefore be required to have policies, procedures and controls to address certain risks including operational, custody, liquidity, investment and credit risk.²⁸ We plan to revisit such exemptions in the future, as the space continues to develop and evolve.

Some Platforms may operate a non-custodial (decentralized) model where the transfer of crypto assets that are securities or derivatives occurs between the two parties of a trade on a decentralized blockchain protocol (e.g. smart contract). These types of Platforms will be required to have controls in place to address the specific technology and operational risks of the Platform.

Consultation questions

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.
21. What other risks are associated with clearing and settlement models that are not identified here?

5.2.8 Applicable regulatory requirements

Platforms that are marketplaces are subject to existing marketplace regulatory requirements, including those summarized at **Appendix B**. Some of these requirements may not be relevant for Platforms and others may need to be tailored to address specific risks.

Platforms may perform additional functions typically performed by dealers and clearing agencies. We are also considering how the requirements summarized at **Appendices C** and **D** may apply. Leveraging the existing regulatory frameworks will ensure that Platforms are treated similarly to

²⁷ Part 13 of NI 21-101.

²⁸ If not already addressed by rules applicable to IIROC Members, to the extent they apply.

other marketplaces, but with appropriately tailored requirements that are relevant for the functions they perform.

Please note that Appendices B, C and D provide only an overview of certain requirements and therefore they should not be relied upon as exhaustive lists of the requirements applicable to marketplaces, dealers and clearing agencies.

Consultation question

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

PART 6 – Providing Feedback

The CSA Regulatory Sandbox is an initiative of the CSA to support business seeking to offer innovative products, services and applications in Canada. The CSA Regulatory Sandbox is a part of the CSA's 2016-2019 Business Plan's objectives to gain a better understanding of how fintech innovations are impacting capital markets and assess the scope and nature of regulatory implications.²⁹

We invite interested parties to make written submissions on the consultation questions identified throughout this Consultation Paper. A complete list of the consultation questions referred to throughout this paper is provided in **Appendix A**. We also welcome you to provide any other comments on the appropriate regulation of Platforms. The information provided will assist us in refining the Proposed Platform Framework and our understanding of this area of innovation.

Please submit your comments in writing by **May 15, 2019**. Please send your comments by email in Microsoft Word format. Address your submission to IIROC and all members of the CSA as follows:

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

²⁹ CSA Business Plan, 2016-2019: https://www.securities-administrators.ca/uploadedFiles/General/pdfs/CSA_Business_Plan_2016-2019.pdf

Please deliver your comments **only** to the addresses below. Your comments will be distributed to IIROC and the other CSA members.

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iroc.ca

Certain CSA regulators require publication of the written comments received during the comment period. We will publish all responses received on the websites of the Autorité des marchés financiers (www.lautorite.qc.ca), the Ontario Securities Commission (www.osc.gov.on.ca), and the Alberta Securities Commission (www.albertasecurities.com). Therefore, you should not include personal information directly in comments to be published. It is important that you state on whose behalf you are making the submission.

PART 7 – Questions

Please refer your questions to any of the following CSA and IIROC staff:

<p>Amanda Ramkissoon Fintech Regulatory Adviser, OSC LaunchPad Ontario Securities Commission aramkissoon@osc.gov.on.ca</p>	<p>Ruxandra Smith Senior Accountant, Market Regulation Ontario Securities Commission ruxsmith@osc.gov.on.ca</p>
<p>Timothy Baikie Senior Legal Counsel Market Regulation Ontario Securities Commission tbaikie@osc.gov.on.ca</p>	<p>Serge Boisvert Senior Policy Advisor Exchanges and SRO Oversight Autorité des marchés financiers serge.boisvert@lautorite.qc.ca</p>
<p>Marc-Olivier St-Jacques Senior Policy Advisor Supervision of Intermediaries Autorité des marchés financiers marco.st-jacques@lautorite.qc.ca</p>	<p>Denise Weeres Director, New Economy Alberta Securities Commission denise.weeres@asc.ca</p>
<p>Katrina Prokopy Senior Legal Counsel, Market Regulation Alberta Securities Commission katrina.prokopy@asc.ca</p>	<p>Sasha Cekerevac Senior Analyst, Market Structure Alberta Securities Commission sasha.cekerevac@asc.ca</p>
<p>Dean Murrison Director, Securities Division Financial and Consumer Affairs Authority of Saskatchewan dean.murrison@gov.sk.ca</p>	<p>Zach Masum Manager, Legal Services, Capital Markets Regulation British Columbia Securities Commission zmasum@bcsc.bc.ca</p>
<p>Ami Iaria Senior Legal Counsel, Capital Markets Regulation British Columbia Securities Commission aiaria@bcsc.bc.ca</p>	<p>Peter Lamey Legal Analyst, Corporate Finance Nova Scotia Securities Commission peter.lamey@novascotia.ca</p>
<p>Chris Besko Director, General Counsel The Manitoba Securities Commission chris.besko@gov.mb.ca</p>	<p>Wendy Morgan Deputy Director, Policy Financial and Consumer Services Commission (New Brunswick) wendy.morgan@fcnb.com</p>
<p>Victoria Pinnington Senior Vice President, Market Regulation IIROC vpinnington@iiroc.ca</p>	<p>Sonali GuptaBhaya Director, Market Regulation Policy IIROC sguptabhaya@iiroc.ca</p>

APPENDIX A

Consultation Questions

1. Are there factors in addition to those noted in Part 2 that we should consider?
2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?
3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?
4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?
7. What factors should be considered in determining a fair price for crypto assets?
8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?
9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?
13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?
16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?
19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.
21. What other risks could be associated with clearing and settlement models that are not identified here?
22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

APPENDIX B

Summary of Regulatory Requirements Applicable to Marketplaces

Marketplaces are subject to the Marketplace Rules and NI 23-103. These include high-level principles relating to access to the marketplaces and trading on the marketplaces. A summary of the regulatory requirements is included below. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to marketplaces.

1. Market integrity

The Marketplace Rules and NI 23-103 have a number of requirements covering market integrity. For example, NI 21-101 requires a marketplace to take reasonable steps to ensure it operates in a way that does not interfere with fair and orderly markets.³⁰ NI 23-101 and securities legislation in some jurisdictions also prohibit any person or company from engaging in transactions that they know, or should know, result in market manipulation or are fraudulent. NI 23-103 also has requirements for marketplaces aimed at maintaining market integrity. For example, marketplaces are required to assess, on a regular basis, whether they require risk management and supervisory controls, policies and procedures, in addition to those of their participants. Marketplaces are also required to assess on a regular basis the continuing adequacy and effectiveness of these controls, policies and procedures.³¹

While the Marketplace Rules and NI 23-103 establish the high-level principles for marketplaces that trade in Canada, the specific requirements applicable to participants on a marketplace are included in the UMIR, which are administered by IIROC.

2. Transparency of operations

Marketplaces are required to make transparent, on their websites, a description of how their orders are entered, interact and are executed, the hours of operation, their fees (including fees for facilitation, routing and mark-ups, if applicable), their affiliates' fees, access requirements, conflicts of interest policies and procedures, and referral arrangements between the marketplace and service providers.³² The purpose of these requirements is to ensure that market participants understand how the marketplace works, as well as the associated risks, its features and its fees.

3. Transparency of orders and trades

Except in certain circumstances, marketplaces must make transparent their order and trade information for securities traded on a marketplace by providing it to an information processor.³³ The information processor collects, consolidates and disseminates their data, and also sets the requirements for the order and trade information that must be provided to it by marketplaces.

4. Transparency to regulators

Marketplaces are required to provide certain information to the securities regulators, so that they

³⁰ s. 5.7 of NI 21-101.

³¹ Part 4 of NI 23-103.

³² s. 10.1 of NI 21-101.

³³ Part 7 of NI 21-101 and Part 8 of NI 21-101 for equity and fixed income securities, respectively.

understand the business of the marketplace and the risks it introduces to the market. Such information is described in the exhibits included in Forms 21-101F1 *Information Statement Exchange or Quotation and Trade Reporting System* and 21-101F2 *Information Statement Alternative Trading System*, for exchanges and ATSS respectively, and relates to: governance, marketplace operations, outsourcing arrangements, systems, custody, the types of securities traded, how access to services is provided, and fees. These forms must be filed prior to the commencement of the operations and must be kept up to date. Changes to the information included in these forms must also be reported to the securities regulators, either in advance, if the change is significant, or subsequent to its implementation if it is not.

In addition, marketplaces report their trading activities on a quarterly basis.³⁴ The quarterly reports are provided to the securities regulators in electronic form. The information reported is included in Form 21-101F3 *Quarterly Report of Marketplace Activities* and includes trading activity information (value, volume and number of trades) by category of security, information about orders and order types, and information about the most traded securities.

5. Listing securities

Exchanges may list securities of an issuer.³⁵ They are required to comply with the fair access requirements in NI 21-101 (and in their recognition orders), which include the requirement to establish written standards for granting access to each of their services,³⁶ including listings. Since exchanges have listings requirements in the form of rules, they must ensure that these rules require compliance with securities legislation³⁷ and that they provide appropriate sanctions for violations of the rules.³⁸

6. Fair access

Marketplaces must not unreasonably prohibit or limit access by a person or company to services offered by the marketplace. A marketplace must establish written standards for granting access to each of its services and must keep records of each access grant or denial of access.³⁹ It must neither permit unreasonable discrimination among participants, issuers and marketplace participants nor impose any burden on competition that is not reasonably necessary and appropriate.⁴⁰ Lastly, a marketplace must not prohibit, condition or otherwise limit a marketplace participant from trading on any marketplace.⁴¹

7. Conflict of interest

A marketplace must establish, maintain and ensure compliance with policies and procedures that identify and manage any conflicts of interest arising from the operation of a marketplace or the

³⁴ Part 3 of NI 21-101.

³⁵ An issuer is listed when there is a formal arrangement between the exchange and the issuer to have the issuer's securities listed, and the exchange has and enforces listing requirements.

³⁶ para. 5.1(2)(a) of NI 21-101.

³⁷ para. 5.3(b) of NI 21-101.

³⁸ para. 5.4(b) of NI 21-101.

³⁹ s. 5.1 of NI 21-101.

⁴⁰ ss. 5.1(3) of NI 21-101.

⁴¹ s. 5.1 of NI 21-101.

services it provides, and any conflicts that owners of the marketplace may have.⁴² These policies must be disclosed on the marketplace's website.

8. Outsourcing

A marketplace that outsources key services or systems to a service provider must have policies and procedures relating to the selection of the service provider, must maintain access to the books and records of the service provider, must ensure that the securities regulatory authorities have access to data that is maintained at the service provider and must review, on a regular basis, the performance of the service provider.⁴³ The outsourcing requirements seek to ensure that the marketplace retains responsibility and control over the outsourced services or systems.⁴⁴

9. Confidential treatment of trading information

A marketplace must not release the order or trade information of any of its participants. This requirement protects each marketplace participant's trading history and strategy. There is an exception to this requirement in limited situations, where data is used for capital markets research and provided certain conditions are met.⁴⁵

10. Recordkeeping requirements

Marketplaces are required to keep books, records and other documents that are reasonably necessary for the proper recording of its business in electronic form.⁴⁶

11. Systems and business continuity planning

Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber attacks. A marketplace is also required to maintain business continuity and disaster recovery plans. A marketplace is required to develop, maintain and test a business continuity plan to ensure uninterrupted provision of key services. A marketplace is required to engage a qualified third party to conduct an independent system review to assess whether it has adequate internal and information technology controls and if they function as designed.⁴⁷

12. Clearing and settlement

All trades executed on a marketplace must be reported and settled through a clearing agency.⁴⁸ Marketplace participants have a choice as to the clearing agency that they would like to use for the clearing and settlement of their trades, provided that the clearing agency is appropriately regulated in Canada.

⁴² s. 5.11 of NI 21-101.

⁴³ s. 5.12 of NI 21-101.

⁴⁴ *Ibid.*

⁴⁵ s. 5.10 of NI 21-101.

⁴⁶ Part 11 of NI 21-101.

⁴⁷ Part 12 of NI 21-101.

⁴⁸ Part 13 of NI 21-101.

APPENDIX C

Summary of Regulatory Requirements Applicable to Dealers

Registration is required if a person or company is in the business of or is holding itself out as being in the business of, trading securities. We have generally found Platforms that intermediate trades of securities between buyers and sellers to be “in the business” of trading securities and subject to the registration requirements set out in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations*, and, where applicable, IIROC Dealer Member Rules and UMIR.

Although the details of the specific requirements applicable to different categories of dealers vary, the summary below captures the basic requirements applicable to a dealer. Please note that this summary should not be relied upon as an exhaustive list of the requirements applicable to dealers.

1. Proficiency

Dealers are in the business of buying and selling securities and derivatives on behalf of the clients and are implicitly or explicitly holding themselves out as having a certain level of knowledge or expertise. Accordingly, individuals registered as dealing representatives are expected to have the education, training and experience that a reasonable person would consider necessary to perform their activities competently, including understanding the structure, features and risks of each security the individual recommends.⁴⁹

Similarly, firms are required to employ individuals as ultimate designated persons (**UDP**) and chief compliance officers (**CCO**) who meet certain additional educational and experience requirements and who will have responsibilities respecting promoting compliance with securities legislation and establishing and monitoring policies and procedures designed to assess compliance by the firm and its dealing representatives with securities legislation.⁵⁰

2. Books and records

Dealers may hold the assets of and conduct transactions on behalf of a multitude of clients. Accordingly, it is important that they maintain books and records that accurately reflect their business activities, financial affairs and client transactions. These books and records requirements help dealers ensure that they are able to prepare and file financial information, determine their capital adequacy, and generally demonstrate compliance with the capital and insurance requirements, among other securities law requirements.⁵¹ Maintaining proper books and records allows dealers to document information about their relationships with their clients and with other entities, as well as, to report to their clients the trades they have transacted on behalf of their clients.⁵²

⁴⁹ The proficiency requirements for registered individuals at investment dealers are set out in IIROC Dealer Member Rule 2900 *Proficiency and Education*. The requirements for registered individuals at dealers other than investment dealers are included in Part 3 of NI 31-103.

⁵⁰ s. 11.2 and 11.3 of NI 31-103, respectively.

⁵¹ s. 11.5 of NI 31-103.

⁵² s. 14.12 and 14.14 of NI 31-103.

3. Compliance system

Given the significant role registered dealers play vis-à-vis their clients and to the capital markets, dealers are required to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to provide reasonable assurance that the firm and each individual acting on its behalf complies with securities legislation and to manage the risks associated with its business in accordance with prudent business practices.⁵³ An effective compliance system includes internal controls and day-to-day monitoring and supervision elements that are appropriately documented. These elements are intended to ensure the integrity of the practices of the dealer, as well as the appropriate segregation of key duties and functions, and includes employee proficiency and training.

As part of a compliance system, a registered firm must appoint both a CCO and an UDP. The CCO is responsible for monitoring, updating and reviewing policies and procedures a registered firm must have as part of its compliance system. The UDP promotes compliance with securities legislation and sets the tone for firm-wide compliance. Investment dealers are also required to appoint a Chief Financial Officer.

4. Financial condition and required capital

Dealers may have access to the assets of a multitude of clients and the insolvency of a dealer could have serious implications for clients and confidence in the capital markets. Accordingly, firms are subject to ongoing financial requirements.⁵⁴

Registered firms are required to calculate regulatory capital to ensure that it is not less than zero. The minimum capital for an exempt market dealer and a restricted dealer is \$50,000 (unless an alternative minimum is imposed). Investment dealers are required to maintain risk adjusted capital, calculated in accordance with IROC requirements, that is greater than zero.⁵⁵

5. Insurance

Similarly, because of the significance of the financial condition of registered dealers to their clients and the capital markets, registered dealers must also maintain bonding or insurance that contains certain specific clauses and coverage. The amount of insurance coverage depends on the category of dealer involved.⁵⁶

6. Financial reporting

Securities regulators monitor the financial condition of registered firms by requiring them to prepare and deliver to regulators annual and interim financial information, and to abide by requirements in IROC Dealer Member Rule 16 *Dealer Members' Auditors and Financial Reporting*.

⁵³ s. 11.1 of NI 31-103.

⁵⁴ The financial requirements for investment dealers are found in IROC Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Form 1. The financial requirements for dealers other than investment dealers are in s. 12.1 of NI 31-103.

⁵⁵ Part 12, Division 1 of NI 31-103.

⁵⁶ The insurance requirements for dealers other than investment dealers are included in s. 12.3 of NI 31-103. The insurance requirements for investment dealers are in IROC Rule 400 *Insurance*.

7. KYC and suitability

Know-your-client and suitability obligations require dealers to collect information to establish the identity of their clients, to understand their investment needs and objectives, overall financial circumstances, and risk tolerance and to then take reasonable steps to use that information to ensure a proposed transaction is suitable to the client. In order to make that suitability assessment, the dealer also needs to understand the features and risks of the security or derivative to be transacted (the know-your-product requirement).⁵⁷ In addition, dealers also have separate, specific obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the associated regulations, including the requirement to verify the identity of clients for certain activities and transactions.

8. Conflicts of interest

Dealers are faced with many potential conflicts of interest between their and their clients' interests. Accordingly, securities legislation requires that a dealer take reasonable steps to identify conflicts of interests that exist and may exist between itself and its clients. Among other requirements, a dealer must identify conflicts of interest that should be avoided and respond appropriately to other conflicts of interest given the level of risk each conflict raises (e.g. through control and/or disclosure of the conflict of interest).⁵⁸

9. Custody

As dealers may have access to clients' assets, there are a number of requirements and prohibitions regarding custody of client cash and securities. Investment dealers, as IIROC members, must comply with the custodial requirements of IIROC.⁵⁹ Depending on the location where such assets are held, investment dealers may have to provide additional capital to reflect increased risk.⁶⁰ Exempt market dealers must comply with the requirements regarding holding client cash and securities set out in NI 31-103 which prohibits them from holding client assets and acting as custodians themselves.⁶¹ Instead, client assets of exempt market dealers are normally held by a custodian that is a separate legal entity.

10. Best execution and fair pricing

Investment dealers are required to establish, maintain and follow written policies and procedures that are reasonably designed to achieve best execution when acting for a client.⁶² What constitutes "best execution" varies depending on the particular circumstances and, for transactions that are executed over the counter, such as transactions in fixed income securities, the expectation is that dealers have policies and procedures to ensure that prices to their clients for these securities are fair and reasonable, both for the pricing of principal transactions and for commissions that may be charged by the dealer.

⁵⁷ The suitability requirements for dealers other than investment dealers are included in Part 13 of NI 31-103. The requirements for investment dealers are in IIROC Rule 1300 *Supervision of Accounts*.

⁵⁸ s. 13.4 of NI 31-103.

⁵⁹ IIROC Dealer Member Rule 2000 *Segregation Requirements*, Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Dealer Member Rule 2600 *Internal Control Policy Statements*.

⁶⁰ IIROC Form 1 General Notes and Definitions, (d) "acceptable securities locations".

⁶¹ s. 14.5.2 of NI 31-103.

⁶² IIROC Dealer Member Rule 3300 *Best Execution of Client Orders*.

11. Handling Complaints

Dealers are required to document complaints and to effectively and fairly respond to them. These procedures should include monitoring of complaints, to allow the detection of frequent and repetitive complaints made with respect to the same matter, which may, on a cumulative basis, indicate a serious problem. Registered firms are required to be a member of the Ombudsman for Banking Services and Investments,⁶³ except in Québec where the dispute resolution service is administered by the Autorité des marchés financiers.

⁶³ Part 13, Division 5 of NI 31-103.

APPENDIX D

Requirements Applicable to Clearing Agencies

A clearing agency is defined in securities legislation as a person or company that, among other activities, provides centralized facilities for clearing and settlement of transactions in securities or, in some jurisdictions, derivatives.

National Instrument 24-102 *Clearing Agency Requirements* (NI 24-102) sets out certain requirements in connection with the application process for recognition as a clearing agency or exemption from the recognition requirement. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to clearing agencies.

NI 24-102 also sets out the ongoing requirements applicable to recognized clearing agencies. This includes the requirement to meet or exceed applicable principles as set up in the April 2012 report *Principles for financial market infrastructures* published by the Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (PFMI). The PFMI cover all areas associated with activities carried out by a clearing agency: systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risk and operational risk. Clearing agencies are required to:

- have appropriate rules and procedures on how transactions are cleared and settled, including when settlement is final;
- minimize and control their credit and liquidity risks;
- have rules that clearly state their obligations with respect to the delivery of securities traded; and
- identify, monitor and manage the risks and costs associated with the delivery of crypto assets, including the risk of loss of these crypto assets.