Raymond Chabot Grant Thornton

May 14, 2019

Raymond Chabot Grant Thornton LLP
Suite 2000
National Bank Tower
600 De La Gauchetière Street West
Montréal, Quebec
H3B 4L8

T 514-878-2691

Investment Industry Regulatory Organization of Canada
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

Via email to: consultation-en-cours@lautorite.qc.ca, comments@osc.gov.on.ca and vpinnington@iiroc.ca

Subject: Comments on Consultation Paper 21-402

We are pleased to have the opportunity to provide our input on the joint Canadian Securities Administrators (CSA)/Investment Industry Regulatory Organization of Canada (IIROC) Consultation Paper 21-402, *Proposed Framework for Crypto-Asset Trading Platforms* (hereafter "CP 21-402").

We believe that CP 21-402 raises issues important to investor protection and public policies. It is an important step in informing the proposed platform framework, and we encourage the CSA and IIROC to move forward with this project and to clarify the rules applicable to participants in the crypto-asset market.

Based on Part 2 of CP 21-402, we understand that the CSA is evaluating how trading occurs on platforms to assess whether or not a security or derivative may be involved. To further refine the factors listed, the CSA may consider recent guidance[1] issued by the US Financial Crimes Enforcement Network (FinCEN) regarding the application of regulations to certain business models involving convertible virtual currencies.

As discussed in Part 4 of CP 21-402, different jurisdictions are taking different approaches to regulating platforms. We encourage the CSA and IIROC to work with

[1] FinCEN Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 2019): https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

regulatory and self-regulatory bodies in other jurisdictions whenever possible to promote the consistency of requirements applicable to platforms. We believe that this consistency is key to minimize regulatory arbitrage, for Canadian-based platforms to be on a level playing field, and to allow Canadian investors appropriate access to this new asset class.

We believe that auditors have a key role to play in enhancing the trust in the crypto-asset market, including in response to the risks mentioned in Part 3 of CP 21-402. As auditors, we feel it is most appropriate for us to only provide input on questions 4 and 5 in section 5.2.1 of CP 21-402. Please find our detailed responses in the appendix to this letter.

Should you wish to discuss any of our comments, please contact the undersigned persons at roy.louis@rcgt.com or trepanier.jean-francois@rcgt.com.

Yours sincerely,

Louis Roy, CPA, CA

Jean-François Trépanier, CPA, CA

Appendix

- **Question 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.**

  We observe that instead of mandating the use of a specific set of standards to mitigate the risks related to safeguarding investors' assets, it may be preferable to provide platforms with flexibility regarding the standards they adopt. We note that a similar approach is currently used in securities regulation. For example, section 3.4 in NI 52-109 respecting certification of disclosure in issuers' annual and interim filings requires the use of a control framework to design the issuer's ICFR but without mandating a specific framework. Section 5.1 in Policy Statement to NI 52-109 provides examples of suitable frameworks.

  It could be required that the standards adopted by platforms exhibit certain characteristics to ensure that they are of high quality. Characteristics could be based on those used in determining the suitability of criteria when conducting engagements in accordance with CSAE 3000[2] or CSAE 3416[3] (i.e., characteristics of relevance, completeness, reliability, neutrality and understandability).

  We believe that a flexible approach can result in a better outcome by allowing bodies of experts to suggest new standards that are more "fit for purpose" for custody of crypto-assets and by updating such standards as necessary. We observe that bodies of experts are already working on standards, including the "CryptoCurrency Security Standard (CCSS)" proposed by the CryptoCurrency Certification Consortium[4] (C4) or the "ISO/NP TR 23576, *Blockchain and distributed ledger technologies – Security management of digital asset custodians*" currently under development by ISO/TC 307. We encourage the CSA and IIROC to monitor and, if appropriate, to participate in the activities of these and other bodies of experts. The CSA and IIROC may also consider forming or supporting a body of Canadian experts in developing standards codifying best practices for custody of crypto-assets.

- **Question 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?**

  We strongly believe that assurance reports issued by independent auditors have an important role in the management of risks associated with custody of crypto-assets, including the risks mentioned in Part 3 of CP 21-402. We strongly support that the endgame is to require that platforms obtain an assurance report for their custody system and those of any third-party custodians.

  We are however unsure whether the preconditions for an assurance engagement are present for all platforms that would be subject to the proposed platform framework, especially the precondition to expect to be able to obtain the evidence needed to support the practitioner's conclusion. The CSA and IIROC will have to

---

[2] CSAE 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*.

[3] CSAE 3416, *Reporting on Controls at a Service Organization*.

[4] https://cryptoconsortium.org/

make a public policy decision about the acceptability of platforms that are not "audit-ready".

CP 21-402 contemplates requiring the platforms to obtain a SOC 2 report. We have the following observations:

- The reason for requiring both a Type I and II is unclear. A Type I report is typically not produced if a Type II exists, because a Type II report contains an opinion on the operating effectiveness of controls (not only their design) and a detailed description of tests of controls performed.
- We encourage the CSA and IIROC to adopt an approach that is flexible regarding the criteria used. A SOC 2 report is based on using the Trust Services Criteria (TSC). The TSC relate to the following trust services principles: security, availability, processing integrity, confidentiality and privacy. While the "security" principle is common to all SOC 2 reports, the other principles are not. If the intent for requiring a SOC 2 report is to achieve comparability between platforms, we believe that it may not be achieved. The TSC can be used to evaluate controls relevant to a variety of different subject matters, and there may also be different interpretations of the applicability of each principle and how characteristics specific to platforms are to be included in the principles and criteria. These differences are more likely to exist when reporting on a new subject matter such as custody of crypto-assets.

  To achieve more consistency, the TSC can be supplemented by other frameworks dealing with a specific subject matter and providing more detailed guidance about the risks and controls For example, in our experience, it is frequent to refer to the National Institute of Standards and Technology (NIST) 800-53 *Cloud Controls Matrix* (CCM) when reporting on cloud solutions.

  While the TSC are widely recognized and offer flexibility in application, they may not be the only suitable criteria for an assurance engagement. As mentioned in our response to question 4, other standards that are more "fit for purpose" for custody of crypto-assets may emerge.
- We believe that a SOC 1 report may also be needed. A SOC 1 report focuses on a service organization's controls that are likely to be relevant to an audit of a user entity's financial statements. When a platform has custody of an entity's crypto-assets, it is likely that certain controls put in place by that platform are part of the entity's information system and are relevant to financial reporting. Information about these controls relevant to financial reporting would be provided by a SOC 1 report, not a SOC 2 report. We note that traditional custodians often make a SOC 1 report available to user entities and their auditors.
- We caution against requiring auditors to report directly to regulators. We note that question 5 refers to "provide assurance to regulators that a Platform has controls in place". We believe that platforms should be held accountable by regulators. SOC reports are typically addressed to management of the entity, and a requirement to address the report directly to a regulator may result in an unwillingness to accept such engagements.