Canadian Securities Law News

January 2020
Number 312

OSC CLEARS PATHWAY FOR THE FIRST PUBLICLY OFFERED BITCOIN FUND

— Carol Derk and Jacqueline Ting. © Borden Ladner Gervais LLP. Reproduced with permission.

On October 29, 2019, the Ontario Securities Commission (OSC) issued reasons for its decision to allow 3iQ Corp. (3iQ), a Canadian investment fund manager, to offer the first publicly offered bitcoin fund in Canada. The OSC Panel ordered that the Director issue a receipt for a final prospectus of The Bitcoin Fund (the Fund), setting aside an earlier decision of the Director to deny the receipt.[1]

The OSC Panel explained that although the concerns about bitcoin expressed by the Director and OSC staff (Staff) had merit, their concerns did not warrant denying a receipt. The OSC Panel's reasons are notable because they provide insight into the OSC's perception of the risks associated with bitcoin, and the regulator's expectations on managers of prospective bitcoin investment funds in recognizing these risks and employing safeguards to mitigate them.

The Fund is a proposed non-redeemable investment fund (NRIF) that would invest substantially all of its assets in long-term holdings of bitcoin purchased from various sources, including bitcoin exchanges. Investors in the Fund would have limited redemption rights – the right to redeem annually at NAV or monthly at a discount to NAV.

The OSC Panel considered two fundamental issues raised by Staff and reflected by the Director's decision:

1. Is bitcoin an "illiquid asset" within the meaning of such term in National Instrument 81-102 *Investment Funds* (NI 81-102), such that the Fund would not comply with the restriction against holding illiquid assets set out in NI 81-102?
2. Would it be in the public interest for the Director to issue a receipt for the Fund's prospectus?

Pursuant to NI 81-102, an NRIF is limited to holding no more than 20 per cent of its NAV in illiquid assets (as defined in NI 81-102). Staff submitted that bitcoin is an illiquid asset because there is no central source for trading data concerning bitcoin. Staff argued that any publicly available trading volume data for bitcoin may be inaccurate and the Fund would have difficulties acquiring or liquidating its assets. As such, Staff argued the Fund would not comply with the illiquid asset restriction in NI 81-102.

However, the OSC Panel accepted 3iQ's evidence of the real volume and trading activities in bitcoin on trading platforms holding a BitLicense (New York State) in large dollar sizes, which 3iQ submitted promote reliable price discovery and provide sufficient liquidity. The

[1] We reported on the Director's decision in our March 2019 bulletin.

OSC Panel concluded that Staff had not demonstrated that bitcoin was an illiquid asset for the purposes of NI 81-102 and, therefore, the Fund could comply with the NI 81-102 restriction against holding illiquid assets.

Staff also argued that it was not in the public interest to issue a receipt for the Fund's prospectus due to concerns about the operational risks inherent in the Fund, including:

1. the Fund's ability to reliably arrive at a NAV given market integrity concerns regarding the trading of bitcoin;
2. the security and safekeeping of the Fund's assets (being bitcoin); and
3. the Fund's ability to prepare and file audited financial statements.

Staff argued that the Fund would not be able to arrive at a NAV that satisfies securities regulatory requirements, citing allegations of price distortion caused by market manipulation in the crypto-asset market, such as wash trading and spoofing.

Although the OSC Panel acknowledged that the risks of price manipulation in the bitcoin market exist, it found that 3iQ mitigated the potential impact on the Fund's valuation because of the Fund's investment parameters and restrictions, as well as its decision to use a specific index to calculate the NAV of the Fund. In particular, the Fund's prospectus states that the Fund would: (i) invest in bitcoin only, not in all crypto-assets; (ii) pursue a buy and hold strategy, not an active trading strategy; and (iii) only buy and sell bitcoin on regulated exchanges.

Staff raised concerns regarding security and safekeeping of the Fund's bitcoin due to security risks associated with crypto-asset trading platforms, such as hacking and insider thefts. Although the OSC Panel recognized the fact that bitcoin can be stolen or lost, it concluded that Staff had not demonstrated that the Fund's bitcoin would be inadequately safeguarded. It referenced several factors in reaching this conclusion, such as the fact that the Fund's proposed custodian and sub-custodian, Cidel Trust Company and Gemini Trust Company, LLC, respectively, are regulated and experienced custodians, and the absence of reliable evidence to suggest that professional, qualified crypto-asset custodians, such as Gemini, have suffered losses of customer assets.

Staff submitted that because Gemini did not currently have a System and Organization Controls of Service Organizations Type 2 report (SOC 2 Type 2 Report)—a customary assurance that Gemini's security controls are working effectively—the Fund's auditor would be unable to complete its report for the Fund's financial statements in accordance with generally accepted auditing standards (GAAS).

The OSC Panel accepted 3iQ's submission that despite the fact that Gemini did not have a SOC 2 Type 2 Report, a qualified auditor could still conduct an audit based on other evidence obtained from third parties and comply with GAAS. Although the Fund may ultimately fail to deliver the required audit report, the OSC Panel noted that Staff would have access to normal course measures to address this deficiency.

The OSC Panel also observed that denying investors the opportunity to invest in bitcoin through a public fund would not promote fair and efficient capital markets and confidence in those markets, but may instead lead to the suggestion that investors should acquire bitcoin through unregulated vehicles. The OSC Panel commented on 3iQ's stated intention to operate and manage the Fund in a prudent manner and to take steps to mitigate against the concerns associated with bitcoin, and remarked that the notion of professionalizing investing in risky assets (through a publicly regulated fund) to mitigate risk should be encouraged.

The OSC Panel concluded that, having considered the risks identified by Staff, ordering the issuance of a receipt for the final prospectus of the Fund was not contrary to the public interest. Contrary to the submissions of Staff, the OSC Panel rejected any notion that terms and conditions be imposed on 3iQ or the Fund noting that it "did not wish to impose conditions that may unduly restrict or constrain 3iQ's ability to exercise its professional judgment" in the matters at hand.

On November 27, 2019, 3iQ filed an updated preliminary prospectus in respect of an initial public offering of units of the Fund, and a receipt for that prospectus was issued on the same day. It will be interesting to see when 3iQ actually launches the Fund and whether investors are convinced that the risks identified by Staff have been properly addressed. We expect that other fund managers may be interested in launching similar investment vehicles now that digital asset funds, or at least bitcoin funds, appear to be permitted in Canada.

Carol Derk is a partner with Borden Ladner Gervais LLP and is a member of BLG's Securities and Capital Markets Group, the National Leader of BLG's Derivatives Group and the Co-National Leader of the Cryptocurrency and Blockchain Group. Carol practises in the area of securities law, specializing in derivatives, investment funds, cryptocurrencies and blockchain. She

works extensively for managers of investment funds, particularly in the area of product development. Carol also has an extensive derivatives practice, including negotiating documentation, advising on regulatory compliance matters and developing new derivatives-based investment products. More recently, Carol has also developed a practice in the blockchain and digital asset space, advising clients that are developing products and services focused on cryptocurrencies and distributed ledger technology. Carol is a regular speaker at seminars and conferences on digital assets, derivatives and investment funds. She is a recipient of the Women's Executive Network (WXN) 2017 Canada's Most Powerful Women: Top 100 Award and is recognized as a leader in her field by Derivatives Week.

Jacqueline Ting is an associate in the Toronto office of Borden Ladner Gervais LLP. Jacqueline practices corporate, commercial and securities law with an emphasis on investment management.

IIROC INTRODUCES MANDATORY REPORTING OF CYBERSECURITY INCIDENTS FOR DEALERS

— Lyndsay A. Wasser, Chiedza Museredza, and Christopher Tworzyanski. © McMillan LLP. Reproduced with permission.

On November 14, 2019, the Investment Industry Regulatory Organization of Canada ("**IIROC**") amended its Dealer Member Rules (the "**Rules**") to require mandatory reporting by dealer members ("**Dealers**") that suffer a cybersecurity incident or breach (the "**Amendments**"). The Amendments are the latest initiative undertaken by IIROC in its ongoing focus on proactively addressing the cybersecurity risk exposure of its Dealers. For this reason, IIROC plans to share the information reported with the Dealer community on an anonymized basis to allow Dealers to understand the nature of risks they face and how they can protect themselves and their clients.

IIROC's mandatory reporting requirements are similar to the requirements of the Office of the Superintendent of Financial Institutions ("**OSFI**") which were introduced earlier this year, and which apply to some Dealers.

However, IIROC's reporting requirements are broader than the reporting requirements under the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), which also apply to some Dealers. IIROC's broader reporting requirements support its mission to protect investors, strengthen market integrity and support healthy Canadian capital markets. You can read more about OSFI reporting requirements in our February 2019 bulletin and PIPEDA reporting requirements in our November 2018 bulletin.

The Amendments require Dealers to report prescribed information regarding a cybersecurity incident to IIROC in two stages:

1. A Dealer must file an initial report with IIROC describing the cybersecurity incident within three (3) calendar days of discovering it;
2. The Dealer must subsequently submit a detailed incident investigation report within thirty (30) calendar days of the incident.

If a Dealer fails to comply with the reporting obligation, IIROC can impose significant monetary penalties or other sanctions.

What Triggers the Reporting Obligation?

A Dealer's reporting obligation is triggered by the Dealer's discovery of a cybersecurity incident.

Cybersecurity incident

Under the Rules, a cybersecurity incident includes any act to gain unauthorized access to, disrupt, or misuse a Dealer's information system, or information stored on such system, which has resulted in, or has a reasonable likelihood of resulting in:

i. substantial harm to any person;

ii. a material impact on any part of the normal operations of the Dealer;

iii. invoking the Dealer's business continuity or disaster recovery plan; or

iv. the Dealer being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization.

IIROC has indicated that the above definition of a cybersecurity incident is intended to be flexible. IIROC expects Dealers to exercise their discretion when determining whether a cybersecurity event meets the reporting threshold.

Dealers should be aware that they are not exempt from the reporting obligation imposed by the Amendments solely because a cybersecurity incident has been experienced by a third-party information systems service provider. Cybersecurity incidents experienced by third parties will trigger a Dealer's reporting obligation if: (i) those third parties are part of that Dealer's "information system"; and (ii) the other elements of the definition of a "cybersecurity incident" are met. We recommend that Dealers consider including provisions in their contracts with the third parties that oblige third parties to: (i) notify Dealers of a cybersecurity incident within 24 hours; and (ii) provide Dealers with all relevant information about the incident. This will help Dealers meet their reporting obligation.

What Information Must be Included in an "Initial Report" and "Incident Investigation Report"?

Initial report

The initial report that is required to be filed by a Dealer within three (3) calendar days of that Dealer's discovery of a cybersecurity incident must include the following information:

i. a description of the cybersecurity incident;

ii. the date on which or time period during which the cybersecurity incident occurred and the date it was discovered by the Dealer;

iii. a preliminary assessment of the incident, including the risk of harm to any person and/or impact on the operations of the Dealer;

iv. a description of the immediate incident response steps the Dealer has taken to mitigate the risk of harm to persons and impact on its operations; and

v. the name and contact information of an individual who can answer any follow-up questions from IIROC on behalf of the Dealer.

IIROC recognizes that a Dealer may not have completed a full analysis of a cybersecurity incident within three (3) calendar days. Accordingly, IIROC does not expect an initial report to reflect material insights respecting the assessment or remediation of a cybersecurity incident. Rather, an initial report is intended to be a preliminary snapshot of the core information relevant to the cybersecurity incident.

Dealers should note that while the information listed above is the minimum information required, IIROC expects Dealers to include additional information about a cybersecurity incident in their initial reports to the extent such additional information is available.

Incident investigation report

An incident investigation report, which is required to be filed by a Dealer within thirty (30) calendar days of that Dealer's discovery of a cybersecurity incident, must include the following information:

i. a description of the cause of the cybersecurity incident;

ii. an assessment of the scope of the cybersecurity incident, including the number of persons harmed and the impact on the operations of the Dealer;

iii. details of the steps the Dealer took to mitigate the risk of harm to persons and impact on its operations;

iv. details of the steps the Dealer took to remediate any harm to any persons; and

v. actions the Dealer has or will take to improve its cybersecurity incident preparedness.

IIROC expects that an incident investigation report will include all relevant and pertinent information that would help a Dealer determine the nature, extent, scope, impact and root cause of a cybersecurity incident. If a Dealer requires more than thirty (30) days to file an incident investigation report, it should notify its IIROC relationship manager.

After filing an initial report, if a Dealer subsequently determines that no cybersecurity incident has occurred, the Dealer does not need to file an incident investigation report. IIROC recommends that Dealers contact external legal counsel and cybersecurity professionals before making such a determination.

How External Legal Counsel Can Assist Dealers in the Event of a Cybersecurity Incident

IIROC recommends that Dealers should follow their incident response and management plan once they discover a cybersecurity incident. If a Dealer does not have an incident response and management plan, IIROC recommends consultation with external legal counsel for assistance to ensure that it protects itself and its clients.

Dealers should be aware that, when a cybersecurity incident occurs, they may be subject to additional reporting requirements under other privacy laws and regulations. External legal counsel can also advise on these other reporting requirements, and assist organizations to meet all applicable legal obligations.

Lyndsay Wasser is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada, and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including privacy and data breaches.

Chiedza Museredza is an associate in McMillan's Privacy & Data Protection and Cybersecurity Group. She advises on a broad range of privacy and cybersecurity issues, including privacy and data breaches.

Chris Tworzyanski is an associate in McMillan's Capital Markets and M&A Group. His practice covers a broad range of matters, including mergers and acquisitions, corporate finance and securities compliance.

RECENT CASES

Sanctions for Fraud

Alberta Securities Commission, November 12, 2019

Vesta Capcorp Inc. ("Vesta") was a federally incorporated company and was also registered in Alberta as an extra-provincial corporation. Brian Arthur Kitts ("Kitts"; together with Vesta, the "Respondents") was Vesta's sole director and guiding mind. Vesta Investors were told that their funds were to be used for short term loans in real estate developments and were promised a 20 per cent return. From February 2014 to June 2015, Vesta raised approximately $5.3 million from 20 investors. The investors' funds were used for unrelated business ventures, by Kitts and his spouse for their personal expenses, and to repay investors as "profits". A substantial amount was lost by the investors. In a decision dated June 3, 2019, a panel of the Alberta Securities Commission (the "Commission") found that the Respondents had engaged in fraud, contrary to paragraph 93(1)(*b*) of the Alberta *Securities Act*, RSA 2000, c. S-4 (the "Act") (the "Merits Decision"; see 2019 CSLR ¶ 900-788). Commission Staff requested various sanctions, including permanent market access restrictions, an administrative penalty of $600,000; and disgorgement of $1,960,457.

The requested sanctions were ordered. The Panel began by noting, among other things, that: sanctions were not meant to punish respondents, but to "prospectively protect investors" and foster "confidence in the integrity of the capital market"; general and specific deterrence and proportionality were to be considered when formulating sanctions (see *Re Cartaway Resources Corp*., 2004 SCC 26); and other factors to consider when fashioning sanctions included the seriousness of the respondent's misconduct, the respondent's characteristics and history, any benefit sought or obtained by the respondent, and mitigating or aggravating circumstances (see *Re Homerun International Inc*., 2016 ABASC 95). Key findings by the Panel included that: fraud was considered one of the most serious contraventions of Alberta securities legislation, and it was particularly egregious that the Respondents engaged in a prolonged Ponzi scheme; Kitts had been found guilty of criminal charges relating to securities fraud and theft in Utah, and was sentenced to imprisonment as a result, but

absconded to Canada to engage in new fraud and was therefore an "unrepenting recidivist"; Vesta obtained approximately $1.9 million (the net of the total obtained from investors less what was returned) and investors were significantly deprived; there were no mitigating circumstances and Kitts' prior criminal record in Utah was an aggravating factor; and, in a similar case involving a Ponzi scheme, the respondent there was permanently prohibited from accessing the market and required to pay an administrative penalty of $500,000. In view of the foregoing, the Panel concluded that permanent market prohibitions were required to deter Kitts and others from engaging in similar misconduct and to protect investors and the market. Turning to the requested disgorgement order, the Panel followed the two-step test set out in *Poonian v. British Columbia Securities Commission*, 2017 BCCA 207: (1) whether the respondent, directly or indirectly, obtained funds as a result of his misconduct; and (2) whether it is in the public interest to make the order. In this case, the evidence presented by Staff established that Vesta had retained approximately $1.9 million, and since Kitts had sole control over Vesta's accounts, the Panel attributed the amounts obtained by Vesta to Kitts. It was also apparent to the Panel that the amounts resulted from the Respondents' fraudulent conduct. The Panel had no trouble in concluding it was in the public interest to order disgorgement, on a joint and several basis, to ensure the Respondents did not get to retain the misappropriated funds. Finally, the Panel also ordered the Respondents to pay an administrative penalty of $600,000, on a joint and several basis, having taken into account the amount ordered to be paid in a similar case.

Re Kitts, 2020 CSLR ¶ 900-809

Appeals of Commission Decisions

British Columbia Court of Appeal, November 14, 2019

Garo Aram Deyrmenjian ("Deyrmenjian") and Raffi Khorchidian ("Khorchidian") were friends, residents of British Columbia, and clients of EHT Corporate Services S.A. ("EHT"), a Swiss wealth management firm. David Craven ("Craven"; together with Deyrmenjian, Khorchidian, and EHT, the "Applicants") was one of the two managing directors of EHT. Kunekt Corporation ("Kunekt") was a Nevada company that had shares quoted on the Over the Counter Bulletin Board market in the United States. During the relevant period, Kunekt was a reporting issuer in British Columbia and had no viable business. Capital Financial Media ("CFM") was a United States entity that was a direct marketer. In November 2010, a total of 13.8 million Kunekt shares were deposited into various offshore accounts (the "Accounts") that Deyrmenjian, Khorchidian, and EHT either indirectly controlled or had beneficial ownership of. Starting in January 2011, CFM commenced a marketing campaign (the "Campaign") which made misleading statements about Kunekt's business prospects (including touting it as the next Apple). As a result of the Campaign, by the summer of 2011, Kunekt's share price rose significantly and Deyrmenjian and Khorchidian sold their beneficially-held shares for profits of approximately $7 million each. CFM issued four invoices for the Campaign. The first three were paid by an account held by EHT, and there was evidence that on the days of the payment of the second and third invoices, amounts close to the sums owed were wired to EHT's account from an account beneficially owned by Khorchidian. The fourth invoice was paid from a Swiss account opened by EHT in the name of a company whose assets were beneficially owned by Khorchidian, and there was evidence that on the day of the invoice's payment, an amount close to the invoice amount was wired from an account of a company whose assets were beneficially owned by Deyrmenjian. In a decision dated April 25, 2018, a Panel of the British Columbia Securities Commission (the "Commission") found that the Applicants had engaged in market manipulation, contrary to paragraph 57(*a*) of the British Columbia *Securities Act,* RSBC 1996, c. 418 (the "Act") (the "Liability Decision"; see 2018 CSLR ¶ 900-734). In particular, the Panel found that: Khorchidian, Deyrmenjian, and EHT, at a minimum, permitted transfers from some of the Accounts to pay invoices from CFM, and thereby contributed to the artificial price; Khorchidian and Deyrmenjian knew, or ought reasonably to have known, that their funding of the Campaign would result in the artificial price for the Kunekt shares, as they knew the company had no real business and they experienced substantial trading gains; and, with respect to EHT, Craven "authorized, permitted or acquiesced" in EHT's conduct, and was also found to have breached paragraph 57(*a*) of the Act. During a subsequent hearing, a Commission Panel dismissed an application under section 171 of the Act by Craven and EHT to revoke or vary the findings in the Liability Decision, and ordered sanctions against the Applicants, including permanent market participation bans, disgorgement by Deyrmenjian and Khorchidian of the proceeds from their sales of Kunekt shares, and significant administrative penalties (the "Sanctions Decision"; see 2019 CSLR ¶ 900-777). The Applicants applied to the British Columbia Court of Appeal (the "Court") for leave to appeal the Liability and Sanctions Decisions pursuant to subsection 167(1) of the Act.

The applications were allowed. The Court began by noting that the applicable principles where leave was sought to appeal a tribunal decision were outlined in *Queens Plate Development Ltd. v. Vancouver Assessor*, Area 09 (1987), 16 BCLR (2d) 104, and included whether: "the proposed appeal raised a question of general importance as to the extent of jurisdiction of the tribunal appealed from"; the appeal was limited to questions of law involving the application of statutory provisions, statutory interpretation important to the applicant, and interpretation of standard wording; there was a marked difference of opinion in the decisions and merit in the issue put forward; there was some prospect of the appeal succeeding with substantial questions to be argued; there was any benefit derived from the appeal; and, the issue on appeal was considered by other appellate bodies. The Court also noted that: the absence of a question of law does not always prevent leave from being granted (see *Grosvenor Canada Limited v. South Coast British Columbia Transportation Authority*, 2015 BCCA 304); a question of what inference a tribunal should draw from proven fact does not raise a question of law, but "the making of an inference based on conjecture or speculation amounts to an error of law (see *R. v. White* (1994), 89 CCC (3d) 336 (NSCA))"; and inferences drawn by a commission are reviewed deferentially, but appellate courts can interfere if the inference drawn amounted to speculation or conjecture (see *ICBC v. Atwal,* 2012 BCCA 12). In the Court's view, EHT's and Craven's appeals raised questions of importance as to the jurisdiction of the Commission over them. Specifically, the determination of whether there was a real and substantial connection between them and British Columbia The Court also found it was a question of general importance as to whether the Liability Decision findings were based on conjecture and speculation as opposed to being "established by clear, convincing and cogent evidence." The Court did not find it appropriate to allow the appeals by EHT and Craven of the Sanctions Decision findings, except to the extent of asserting that the sanctions should be set aside if their appeals were allowed. In the Court's view, the Commission's reasoning in the Sanctions Decision was sound, it was owed deference, and the appeals did not raise questions of law. Turning to Khorchidian and Deyrmenjian, the Court was less inclined to grant their appeals of the Liability Decision on the basis that, while they raised questions of general importance and law, there was evidence that they profited from the Campaign. However, the Court concluded it would allow their applications as the same legal issues would be raised in the appeals of EHT and Craven and there would be a risk of delay if the Deyrmenjian and Khorchidian applications were not allowed. Second, there could be embarrassment as findings from the EHT and Craven appeals could impact inferences drawn by the Commission against Khorchidian and Deyrmenjian. The Court limited Khorchidian's and Deyrmenjian's appeals of the Sanctions Decision for the same reason as EHT's and Craven's were limited.

Khorchidian v. British Columbia Securities Commission, 2020 CSLR ¶ 900-810

Sanctions for Breach of a Cease-Trade Order

British Columbia Securities Commission, November 4, 2019

EcoTECH Energy Group Inc. ("ecoTECH") was a Nevada corporation with its shares quoted on the over-the-counter market in the United States, and it was a reporting issuer in British Columbia. Colin V. Hall ("Hall"), Rolf Eugster ("Eugster"), and Anne Sanders ("Sanders"; together with Eugster, Hall, and ecoTECH, the "Respondents") were all British Columbia residents who held various executive positions with ecoTECH. On July 17, 2012, the Executive Director of the British Columbia Securities Commission (the "Commission") issued a cease-trade order (the "Order") which required that all trading in ecoTECH securities cease as it was not in compliance with its disclosure obligations. Between December 2012 and December 2013, the Respondents breached the Order when ecoTECH issued 2,009,634 shares to 16 investors (the "Cash Investors") for cash proceeds of $55,100. A further 73 million shares were issued to 15 persons as compensation for services rendered to ecoTECH at a price of $0.045 per share. In a decision dated June 3, 2019, a Commission Panel found that: ecoTECH breached the Order and made misrepresentations to the Cash Investors, contrary to paragraph 50(1)(*d*) of the British Columbia *Securities Act,* RSBC 1996, c. 418 (the "Act"); and, pursuant to section 168.2 of the Act, as directors or officers of ecoTECH, Hall, Eugster, and Sanders also breached the terms of the Order and made misrepresentations (see 2019 CSLR ¶ 900-787). The Executive Director sought an order for various sanctions, including: broad market prohibitions against the individual respondents for five years; payment of a $20,000 administrative penalty by each of Sanders and Hall; and payment of a $17,000 administrative penalty by Eugster. No sanctions were sought against ecoTECH which continued to be subject to the Order.

Various sanctions were ordered. The Panel began its analysis by noting, among other things, that, orders are "protective and preventative, intended to be exercised to prevent future harm", and factors to be considered when fashioning sanctions included: the seriousness of the respondent's conduct; the harm to investors and the integrity of the capital

market; the respondent's enrichment and past conduct; mitigating factors; the risk to the market if the respondent continues to participate; the respondent's fitness to be a director, officer, or adviser to issuers; specific and general deterrence; and orders made in similar cases (see *Re Eron Mortgage Corporation,* [2000] 7 BCSC Weekly Summary 22). Key findings by the Panel included that: cease-trade orders are important tools in protecting the market, and undermining one is therefore serious misconduct (see *Re Loughery,* 2019 BCSECCOM 78), and in this case, the individual respondents were well aware of the Order and still authorized issuance of the ecoTECH shares; the Cash Investors were likely deprived, as the shares were still subject to the Order, and ecoTECH was enriched by their funds; there were no mitigating or aggravating circumstances; the individual respondents posed risks to the market as they demonstrated an unwillingness to comply with regulators; and, in *Loughery, Cinnabar Explorations Inc. (Re),* 2014 BCSECCOM 26, and *Oriens Travel & Hotel Management Corp (Re),* 2014 BCSECCOM 91, cease-trade orders were breached and the respondents (who were personally enriched) were subject to, among other things, six-year market participation bans and fines ranging from $15,000 to $50,000. In light of the foregoing, the Panel determined that a market participation ban of five years was appropriate for Hall and Sanders, and four years for Eugster given his lesser role in the misconduct. The Panel also ordered Hall and Sanders to pay administrative penalties of $20,000, and Eugster to pay $15,000 as proportionate to the misconduct and given the precedents. The individual respondents had argued they were impecunious, and no fines should be ordered, but presented no evidence of the same.

Re ecoTECH Energy Group Inc., 2020 CSLR ¶900-811

Review of a Director's Decision

Ontario Securities Commission, October 29, 2019

The Bitcoin Fund (the "Fund") was to be a public, non-redeemable investment fund that would invest substantially all of its assets in bitcoin, a digital crypto-asset that was not issued by any government or bank, but based on the "decentralized, open source protocol of the peer-to-peer Bitcoin computer network". 3iQ Corp. ("3iQ", together with the Fund, the "Applicants") was to be the Fund's investment fund manager and portfolio manager. 3iQ also managed a private investment fund that invested in crypto-assets. In late 2016, 3iQ began meeting with the Ontario Securities Commission's (the "Commission") Investment Funds & Structured Products branch ("IFSP") regarding its proposed preliminary prospectus for the Fund. IFSP Staff ultimately advised that its recommendation to the Director was not to issue a receipt for the Fund's prospectus. On February 15, 2019, the Director released his decision denying a receipt for the Fund's prospectus on the basis that: bitcoin was an illiquid asset, as defined in National Instrument 81-102 *Investment Funds* ("81-102"), and as such, the Fund would not comply with the restriction against holding illiquid assets set out in section 2.4; and it was not in the public interest to issue the receipt as there were concerns about the Fund's ability to value its assets given market integrity concerns, the security and safekeeping of the Fund's bitcoin, and the Fund's ability to file required audited financial statements (the "Decision"). The Applicants applied to the Commission for an order setting aside the Decision and directing the Director to issue a receipt for the Fund's final non-offering prospectus.

The Director's Decision was set aside and the Director was ordered to issue a receipt. The two main issues before the Panel were: was bitcoin an illiquid asset such that the Fund would not comply with 81-102; and was issuing a receipt for the Fund's prospectus against the public interest? Salient points by the Panel included that: it was "not the role of securities regulators to approve or disapprove of the merits of securities being offered to the public"; regulators were required to ensure broad public interest and balance the principles of the Act, which did not include consumer protection issues; and the burden was on Staff to show a receipt should not be issued for a fund's prospectus. On the first issue, the Panel began by noting that 81-102 restricts the amount of illiquid assets (assets that cannot be readily disposed of through market facilities which use public quotations regarding valuation) due to concerns that illiquid assets are more difficult to value for the purposes of calculating a fund's net asset value. The Panel's conclusion was that Staff failed to establish that bitcoin was an illiquid asset, because, while bitcoin did not trade on market facilities comparable to the Toronto Stock Exchange, the Applicants had provided "sufficient evidence of real volume and real trading in bitcoin on registered exchanges in large dollar size, both in absolute terms and compared to other markets for commodities and equities, which constitutes a liquid market." The Panel noted that some "bitcoin trading platforms and OTC desks [were] regulated by the New York State Department of Financial Services (New York State)." As the Fund was in compliance with 81-102, there was no basis for the denial of a receipt on this ground. On the second argument made by Staff, that there were operational concerns that would make issuance of a receipt contrary to the public interest, the Panel found

that: the Applicants had presented an acceptable means to value the Fund's bitcoin holdings that would permit compliance with National Instrument 81-106 *Investment Fund Continuous Disclosure*; Staff failed to demonstrate that the Fund's bitcoin would be inadequately safeguarded given the Fund's proposed use of qualified custodians and other protective measures; and Staff also failed to establish that an audit report was impossible (the Applicants had flagged in its prospectus that there was a risk it could fail to provide the require audit report, and if that was the case, then Staff could intervene). Having addressed the operational risks (which were all beyond the control of the Applicants), the Panel reviewed the purposes and principles of the Act, and noted, among other things, that: there were no allegations that the Applicants would "engage in unfair, improper or fraudulent practices in their operations and management of the Fund and, in fact, the evidence is to the contrary; the Applicants intend to operate and manage the Fund in a prudent and professional manner"; the Applicants were proposing to take reasonable steps to address operational risks; bitcoin was already available for purchase, and "denying investors the opportunity to invest in bitcoin through a public fund would not promote fair and efficient capital markets and confidence in capital markets"; and refusing to issue the receipt "would be contrary to the principle that business and regulatory costs and other restrictions on the business and investment activities of market participants should be proportionate to the significance of the regulatory objectives sought to be realized". In the Panel's view, capital market participants proposing to deal with innovative and risky assets such as bitcoin should be encouraged to engage with the Commission, as the alternative was for investors to acquire the assets through unregulated vehicles.

Re 3iQ Corp. and the Bitcoin Fund, 2020 CSLR ¶ 900-812

CANADIAN SECURITIES LAW NEWS

Published monthly as the newsletter complement to the *Canadian Securities Law Reporter* and the *Canadian Stock Exchanges Manual* by LexisNexis Canada Inc. For subscription information, contact your Account Manager or call 1-800-387-0899.

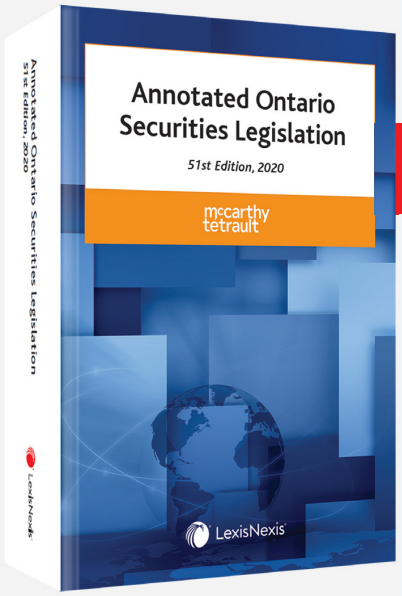
For LexisNexis Canada Inc.

Jaime Latner, LLB,
Content Development Associate
905-479-2665
email: jaime.latner@lexisnexis.ca

Customer Support
Phone: 1-800-387-0899
Email: service@lexisnexis.ca
Customer Service is available from 7 a.m. to 11 p.m. (ET) Monday to Friday, and from 9 a.m. to 11 p.m. (ET) on Weekends.

Notice: *This material does not constitute legal advice. Readers are urged to consult their professional advisers prior to acting on the basis of material in this newsletter.*

LexisNexis Canada Inc.
111 Gordon Baker Road
Suite 900
Toronto, Ontario
M2H 3R1



NEW EDITION

AVAILABLE OCTOBER 2019

$185 | 4,234 pages | Softcover

Semi-Annual | ISBN: 9780433503224

Annotated Ontario Securities Legislation, 51st Edition, 2020

McCarthy Tétrault

This book provides essential information for practitioners dealing with securities laws in Ontario, including full text of the Ontario *Securities Act*, Ontario Securities Commission Rules, Policies, and Notices, National Instruments and Policy Statements, and Rules of Procedure.

What's New in the 51st Edition

- New Joint CSA/IIROC Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms*, published March 14, 2019
- New CSA Staff Notice 21-326 *Guidance for Reporting Material Systems Incidents*, issued March 15, 2019
- New CSA Staff Notice 31-354 *Suggested Practices for Engaging with Older or Vulnerable Clients*, issued June 21, 2019
- New CSA Staff Notice 45-325 *Filing Requirement and Fee Payable for Exempt Distributions involving Fully Managed Accounts*, issued February 7, 2019
- New OSC Staff Notice 11-784 *Burden Reduction*, issued January 14, 2019
- Amendments to OSC Rule 13-502 *Fees*, *OSC Rule 13-503 (Commodity Futures Act) Fees*, and corresponding companion policies, effective July 17, 2019

LexisNexis.ca/ORStore

LexisNexis