Management's Discussion and Analysis

For the Year Ended October 31, 2020
Stated in Canadian Funds

Dated: October 28, 2022

This management's discussion and analysis of the financial condition and results of operation ("MD&A") of NetCents Technology Inc. ("NetCents" or the "Company") should be read in conjunction with NetCents' annual audited consolidated financial statements and notes thereto for the year ended October 31, 2020.

Except as otherwise indicated, all financial data in this MD&A have been prepared in accordance with International Financial Reporting Standards ("IFRS") issued by the International Accounting Standards Board ("IASB") and interpretations of the International Financial Reporting Interpretations Committee ("IFRIC").

The Company's functional and reporting currency is the Canadian dollars and all dollar amounts are in Canadian dollars, unless otherwise indicated.

Discussion of the Company, its operations and associated risks is further described in the Company's filings, available for viewing at www.sedar.com.

## ABOUT THE COMPANY AND BUSINESS OVERVIEW

NetCents is an automated transactional hub for payments that eliminates inefficiencies, provides Instant Settlements, and removes price volatility associated with cryptocurrency payments. NetCents has perfected an easy to use, seamless platform to transact using cryptocurrency that is wallet agnostic therefore easy for any cryptocurrency holder or merchant to access. In addition, the platform is scalable, secure, and automated. The quick and fully automated onboarding process for merchants enables the acceptance of major crypto currencies as payments for goods and services. NetCents removes the volatility risk for merchants by instantly converting the Crypto received into the merchant's choice of fiat currency, and is directly deposited into their bank accounts. The NetCents solution provides the merchant with a guaranteed price, unlimited transaction size and unlimited volumes, while eliminating fraud and chargebacks.

**Merchant Gateway**

The NetCents Gateway is integrated into and is the underlying technology for every layer of the traditional payments ecosystem, including payment gateways, payment processors, Independent Sales Organizations (ISOs), Independent Software Vendors (ISVs), and Point of Sale (POS) platforms and terminals to power their merchants' cryptocurrency transactions.

The merchant gateway supports merchant transactions in-person through POS integrations and the NetCents iOS and Android applications, online through API, hosted payments, and eCommerce plugins, and via email with the virtual terminal or invoicing system.

Merchants have the ability to choose Manual or Instant Settlements. With Manual settlements, merchants choose to keep their transactions in cryptocurrency. Instant Settlements is a guaranteed price protection eliminating the volatility from price swings of accepting cryptocurrency. At the time of the transaction, the NetCents Gateway locks in and guarantees the sale price and the merchant receives the full fiat value of the transaction less the transaction fee.

NetCents is focused on growing its total merchant base in target industries as well as targeted geographic areas. By taking this approach, NetCents is positioning itself as the top gateway choice for small and medium businesses in key growing areas of the world.

NetCents chooses to limit the number of cryptocurrencies to the most popular coins on the market. While competitors may choose to support more niche coins, NetCents remains focused on prioritizing the cryptocurrencies that it believes will enable widespread adoption.

The NetCents Gateway is diligently updated providing the most up to date and secure platform for merchant to transact business. The NetCents Gateway also provides an API that allows merchants to create a custom checkout page. Merchants are provided an easy onboarding process, no start-up fees, monthly fees, or contracts. This along with a simple transactional fee structure offers merchants quick and easy access to new customers paying with cryptocurrency.

NetCents currently generates revenue from,

- Merchant transaction fees are collected from each merchant transaction processed, the standard transaction fee is 1.99% plus $0.05 cents per transaction. On the user portal and NC Exchange, NetCents generates revenue from trades, withdrawals, processing fees, and arbitrage trading; and
- FX revenue from all transactions that happen in all parts of the NetCents ecosystem.

**The NetCents Exchange**

The user portal NetCents Exchange allows NetCents users to buy, sell, and transact with cryptocurrency. Platform features include: cryptocurrency wallet, buying/selling/transacting with cryptocurrency, view live market information and historical prices, iOS and Android applications, multiple methods of fiat onramp and offramp, and multiple fiat and cryptocurrency pairings.

*During the year ended October 31, 2020, some key business development announcements included,*

- On November 5, 2019, The Company announced that it continues to advance on all key metrics that the Company is using to track growth. In October the Company's processing volume was 12% greater than in

September and 7.6 times greater than in February. This growth signals continued increasing demand from both merchants and consumers for cryptocurrency payments as the Company has now processed millions of dollars in cryptocurrency transactions.

- During the year NetCents announced the addition of Ripple (XRP) to the NetCents merchant gateway and Instant Settlement program to allow for purchases at all of our participating merchants.

- During the year NetCents announced that it has begun daily settlements for merchants that exceed $100,000 in monthly cryptocurrency processing volume. Through the Merchant Acquisition Program (MAP) the Company launched in 2019, it has successfully targeted enterprise merchants that exceed the $100,000 monthly threshold for daily settlements. This initiative helped the Company exceed $1 million in monthly processing volume, as announced in January 2020.

- During the year NetCents announced the choice of Lightning Network to Enhance its Payments Backbone. The Lightning Network is a "Layer 2" payment protocol that operates on top of blockchain-based cryptocurrencies, enabling near instant transactions with extremely low or non-existent blockchain fees for users regardless of network congestion. Lightning Network will enable the Company to complete payments off the blockchain and allow the Company to process over 1 million transactions per second.

- During the year the Company announced that it has integrated its platform into the banking Automated Clearing House (ACH) for all US-based merchant payouts. The integration of ACH into the platform decreases the cost of a merchant payout by 80%.

- During the year the Company announced numerous enhancements to its system. NetCents has been running promotional test campaigns, both merchants directly and through Partners to test the efficacy of various promotional incentives in driving merchant sign ups, integration, and the processing of cryptocurrency transactions. Through this testing, it was identified that due to the wide-range of merchant and partner industries, the ability to conduct partner-specific and varied promotions was key to the campaign's ongoing success. NetCents works with its Partners to develop and launch programs that encourage downstream merchants to begin accepting cryptocurrency as a method of payment. To meet increasing and varied demand from its partners on these promotional programs, NetCents has now automated most features of the promotion system so it can manage numerous campaigns simultaneously. Most importantly, Partners now have a toolkit to create customized promotion campaigns that fit their merchant base's needs and requirements.

- During the year NetCents announced that it continues to grow its international merchant base and has begun inroads to new merchant industries, notably Business to Business (B2B). The Company has experienced a rapid geographic diversification of its merchant base in 2020 when compared to 2019. In 2019, 27% of the Company's merchants were located outside of the United States compared to 67% in 2020 with 81% of new merchants using the merchant gateway located internationally.

*Significant events and material transactions announcements subsequent to October 31, 2020, included,*

- The Company has been subject to a management cease trade order since March 4, 2021, when it failed to file its annual financial statements and MD&A for the year ended October 31, 2020 (the "2020 Annual Report") by the regulatory filing deadline. The filing delay was due to complexities related to the audit of cryptocurrency transactions and obtaining insufficient confirmatory balance requests by cryptocurrency account holders. The combination of technical challenges and insufficient accounting staff led to increased delays. On May 7, 2021 trading of the Company's shares on the CSE was halted due to the filing delays. There has been no material change that has not been generally disclosed and the Company has complied with and satisfied the provisions of the alternative information guidelines set out in National Policy 12-203.
- On July 5, 2022, the Company announced it had established a joint venture with Sheikh Mohammed Maktoum Huma Al Maktoum Investment LLC (MBM). MBM has assisted the Company with local sponsorship and licensing in the United Arab Emirates (UAE). Along with the joint venture, the Company announced that it has received a Dubai Economic Department Payment Service Provider (PSP) with the blessing and a review of the Central Bank of the UAE to conduct business. The joint venture included the establishment of NetCents Payment Service Provider LLC (NPSP), a Dubai limited liability company. The Company currently owns 49% of NPSP. The remaining 51% is owned by MBM.
- On August 10, 2022, the Company established NetCents Technology UK Ltd, a UK private limited company. The Company plans to use this wholly owned subsidiary to expand growth in the region.

## FINANCIAL DATA

### *Selected Annual Information*

The following table summarizes selected financial data for the Company for each of the most recently completed financial years. The information set forth below should be read in conjunction with the consolidated audited financial statements and related notes.

| For the year end October 31 | 2020 | 2019 | 2018 |
|---|---|---|---|
| Revenue | $ 271,492 | $ 89,082 | $ 120,578 |
| Net Loss from Operations | $ (21,437,592) | $ (5,575,879) | $ (10,565,991) |
| Net Loss | $ (21,185,271) | $ (6,665,702) | $ (13,193,394) |
| Basic & Diluted Loss Per Share | $ (0.30) | $ (0.14) | $ (0.32) |
| Total Assets | $ 6,661,621 | $ 4,077,710 | $ 6,985,244 |
| Cash Dividend Declared | $ - | $ - | $ - |

### *Results of Operations Analysis for years ended October 31, 2020 versus 2019*

The comprehensive loss for the year ended October 31, 2020 was $21,185,271 which compares to a comprehensive loss of $6,665,702 incurred for the year ended October 31, 2019. The main fluctuations in costs are as follows:

| | | | Variance - Increase (Decrease) | |
|---|---|---|---|---|
| **For the year end October 31** | **2020** | **2019** | **$ Variance** | **% Variance** |
| **Revenue** | **$ 271,492** | **$ 89,082** | **$ 182,410** | **205%** |
| During the year ended October 31, 2020, the Company continued to enter into multiple merchant agreements and continued to generate revenue with its payment processing platform. The variance is attributable to timing of certain transactions. | | | | |
| **Share based compensation** | **$ 9,802,418** | **$ 1,416,939** | **$ 8,385,479** | **592%** |
| During the year ended 31 October 2020, the Company issued substantially more shares, stock options and warrants for services and employment related compensation to directors, officers, consultants and employees. | | | | |
| **Salaries and wages** | **$ 3,170,718** | **$ 593,177** | **$ 2,577,541** | **435%** |
| During the year ended October 31, 2020, the increase in payroll is a result of the Company converting several consultants into employees, and a bonus paid to certain employees. The Company's employees have also increased since then as a result of increase in the Company's market capitalization and operation | | | | |
| **Professional fees** | **$ 1,085,310** | **$ 397,505** | **$ 687,805** | **173%** |
| During the year ended October 31, 2020, ongoing costs related to legal fees incurred in the previous period in connection with regulatory matters as a result of the trading halt in the CSE and it increased the engagement of accounting and compliance specialist to ensure adqueate procedures, risk management planning and reporting structure can be set to scale profitability and efficiently | | | | |
| **Consultant fees** | **$ 5,092,158** | **$ 174,533** | **$ 4,917,625** | **2818%** |
| During the year ended October 31 2020, the company engaged signficantly more consultants for services provided across the operations, primarily in the area of marketing, investor relations and technology development. Such items have be categorize separately so that direct employee salaries can be reflected in noted line items. Depending on how the businesss plan evolves, the Company will look to convert 3rd party consultants into employement as a retention and development strategy | | | | |

### *Financing activities for the year ended October 31, 2020,*

On February 10, 2020, NetCents announced a non-brokered private placement (the "Offering") for up to $100,000. Pursuant to the Offering, the Company issued 357,143 units ("Units") at a Canadian Security Exchange ("CSE") "price protected" rate of $0.28 per unit, for gross proceeds of $100,000. Each Unit consists of one common share of the Company (a "Share") and one common share purchase warrant of the Company (a "Warrant"). Each Warrant entitles the holder to acquire one common share of the Company (a "Warrant Share") at an exercise price of $0.70 for a period of 24 months from the closing date of the Offering.

On June 19, 2020, the Company announced that it entered into an agent and advisory services agreement with Boustead Securities, LLC ("Boustead"), a California limited liability corporation, whereby the Company engaged Boustead to act as the Company's placement agent, on an exclusive basis in North America, with respect to the Company's securities offerings (the "Financings"). In exchange for the services provided by Boustead and, subject to

the approval of the CSE, the Company will issue an aggregate of 250,000 common shares (the "Shares") in the capital of the Company to Boustead at a fair value of $1.85 per Share and to pay Boustead a success fee when the Company closes on a Financing payable as agreed to between the parties.

## *Outstanding Shares*

As October 31, 2020, the Company had 82,660,496 common shares issued and outstanding. As of October 31, 2020, the fully diluted amount of 105,286,404 includes common share purchase warrants 10,928,978 and 8,635,500 options outstanding.

## *Liquidity and Capital Resources*

The consolidated financial statements were prepared on a "going concern" basis, which assumes that the Company will continue in operation for the foreseeable future and will be able to realize its assets and discharge its liabilities and commitments in the normal course of business.

In March 2020 the World Health Organization declared coronavirus COVID-19 a global pandemic. This contagious disease outbreak, which has continued to spread, and any related adverse public health developments, has adversely affected workforces, economies, and financial markets globally, potentially leading to an economic downturn. It has also disrupted the normal operations of many businesses, including the Company's. This outbreak could decrease spending, adversely affect demand for the Company's product and harm the Company's business and results of operations. It is not possible for the Company to predict the duration or magnitude of the adverse results of the outbreak and its effects on the Company's business or results of operations at this time.

Cash used in operating activities totalled $4,135,032 and $2,861,741 for the years ended October 31, 2020 and 2019, respectively.

Cash used in investing activities totalled $8,338 and $0 for the years ended October 31, 2020 and 2019, respectively.

Cash provided by financing activities totalled $5,848,646 and $1,985,536 for the years ended October 31, 2020 and 2019, respectively.

The Company had a working capital surplus (deficiency) of $888,186 and ($2,498,643) for the year ended October 31, 2020 and 2019, respectively.

The Company maintained unrestricted cash of $1,910,364 and $205,088 for the year ended October 31, 2020 and 2019, respectively. The Company maintained unrestricted digital currency of $428,422 and $100,221 for the year ended October 31, 2020 and 2019, respectively.

As of October 31, 2020, the Company had financial obligations to unrelated parties as follows:

- Accounts payable and accrued liabilities of $830,492 and $286,518, respectively versus $1,141,537 and $180,752, respectively as of October 31, 2019;
- Loans payable of $95,406 versus $31,281 as of October 31, 2019;
- Funds due to merchants of $207,717 versus $292,499 as of October 31, 2019; and
- Deposits due to clients of $536,473 versus $1,255,593 as of October 31, 2019

## *Proposed Transactions*

The Company does not have any new or proposed transactions contemplated as of the date of this report.

## *Off-Balance Sheet Arrangements*

The Company had no off-balance sheet arrangements as of October 31, 2020 and as at the date hereof.

## *Related Party Transactions*

*a) Key management compensation*

| Name and Position | Fiscal Period | Dollar based payments | Share based payments |
|---|---|---|---|
| Clayton Moore, CEO and director – salary | **2020** | **$ 269,000** | **$ 414,029** |
| | 2019 | $ 202,000 | $ 79,712 |
| Gord Jessop, former President and director – salary | **2020** | **$** | **$ 16,500** |
| | 2019 | $ 148,500 | $ 79,712 |
| Jennifer Lowther, CRO and director – consulting fees | **2020** | **$ 170,329** | **$ 968,826** |
| | 2019 | $ 113,400 | $ 251,284 |
| Christopher Cherry, CFO and director – consulting fees | **2020** | **$ 127,373** | **$ 120,000** |
| | 2019 | $ 70,875 | $ |
| Mehdi Mehrtash, CTO – salary | **2020** | **$ 220,000** | **$** |
| | 2019 | 90,000 | 78,747 |

*b) Related party transaction and balances*

An amount of $100,008 due from related parties as of October 31, 2019, from a company controlled by former President of the Company was written off in the year as it was deemed uncollectible.

Included in due from related parties as of October 31, 2020, is $426,690 due from the CEO to the Company (versus October 31, 2019, which was due to the CEO of $114,118). These amounts are non-interest bearing with no fixed terms of repayment. On July 29, 2020, the Board of Directors approved a loan to the CEO of the Company in the amount of $361,384. The loan is non-interest bearing and matures one year from the issuance date. During the

year ended October 31, 2021, the CEO repaid all amounts owed. During the year, the CEO advanced $83,500 to the Company through an entity he is sole owner.

During the year ending October 31, 2020, the company entered into a settlement agreement with the CEO of the Company. Under the settlement agreement the CEO received 3,696,205 of the Company's common shares value at $0.19 per share totalling $693,039.

Included in due from related parties as of October 31, 2020, is $69,061 due from the Chief Revenue Officer of the Company (October 31, 2019, which was due to the Chief Revenue Officer of $1,236). These amounts are non-interest bearing with no fixed terms of repayment.

Key management and related parties options, warrants and debt settlement transaction for the year end October 31, 2020 consisted of;

- Christopher Cherry, etal.("CFO") was granted 100,000 warrants at $0.70 and 450,000 options with an exercise price ranging from $0.62 to $1.10. The Company settle a debt obligation with the CFO for $80,850 through the exchange of 380,000 shares with a fair value of $119,200.
- Jennifer Lowther, granted 500,000 options with an exercise price ranging from $0.62 to $1.10.
- Clayton Moore, CEO, options expired 125,000. The Company settle a debt obligation with the CEO of $693,038 through the exchange of 3,696,205 shares with a fair value of $887,089.
- The Company settle a debt obligation with an entity owned by the CEO for $91,562 through the exchange of 327,008 shares with a fair value of $186,395.
- The Company settle a debt oblication with Gord Jessop of $55,458 through the exchange of 270,443 shares with a fair value of $64,906.

## *Commitments*

**a) Commitments with related parties**

Pursuant to the employment agreement, effective August 13, 2020, the Company will remunerate the Chief Executive Officer of the Company $25,000 per month (2019: $18,500). In addition, the CEO shall receive a quarterly bonus equal to 250,000 Class A voting shares of the Company with the value of such shares being determined by the share price of the Company on the last day of the fiscal quarter, less any permissible deduction to the current market price. In the event that the CEO is terminated without cause, the Company must continue paying the salary for a period of 18 months.

Pursuant to the employment agreement, effective August 13, 2020, the Company will remunerate the Chief Revenue Officer (the "CRO") of the Company $18,000 per month. In addition, the CRO shall receive a quarterly bonus equal to 250,000 Class A voting shares of the Company with the value of such shares being determined by the share price of the Company on the last day of the fiscal quarter, less any permissible deduction to the current market price. In the event that the CRO is terminated without cause, the Company must continue paying the base salary for a period of 18 months.

**b) Other commitments**

On 1 March 2018, the Company entered into a premises lease agreement for a period of seven years, expiring on 28 February 2025. Through an assignment of lease agreement dated December 18, 2020, the Company assigned all rights and obligations of this lease to an independent third party. The assignment was made effective as of March 1, 2021.

## *Financial Instruments*

*a) Financial instrument classification and measurement*

Financial instruments of the Company carried on the statement of financial position are carried at amortized cost. There are no significant differences between the carrying value of financial instruments and their estimated fair values as of October 31, 2020, and 2019. There have been no changes in levels during the period.

The Company classifies the fair value of these transactions according to the following hierarchy:

- Level 1 – quoted prices in active markets for identical financial instruments.
- Level 2 – quoted prices for similar instruments in active markets; quoted prices for identical or similar instruments in markets that are not active; and model-derived valuations in which all significant inputs and significant value drivers are observable in active markets.
- Level 3 – valuations derived from valuation techniques in which one or more significant inputs or significant value drivers are unobservable.

*b) Fair values of financial assets and liabilities*

The Company's financial instruments include cash, restricted cash, and funds due from processors, cash included in assets held for clients, due to related parties, accounts payable and accrued liabilities, client deposits, loans payable and funds due to merchants. As October 31, 2020, and 2019, the carrying value of cash and certain assets held for clients and client deposits are at fair value. The remaining financial instruments approximate their fair value due to their short-term nature.

The Company may not be able to realize the economic benefit of a hard fork or airdrop, either immediately or ever, for various reasons. For instance, the Company may not have any systems in place to monitor or participate in hard forks or airdrops. Therefore, the Company may not receive any new cryptocurrencies created as a result of a hard fork or airdrop, thus losing any potential value from such cryptocurrencies.

## RISKS AND UNCERTAINTIES

The risks and uncertainties described below and elsewhere in this MD&A are the principal risks to which the Company is exposed, which may materially affect the Company's business, financial condition, results of operations, cash flows, future prospects or the trading price of its common shares. Such risks and uncertainties are those management currently believes to be material, but they are not the only ones that the Company faces. If additional risks and uncertainties not presently known to us or that we currently believe to be immaterial actually occur or become material risks, our business, prospects, financial condition and financial performance could be materially and adversely affected. Further reference should be made to the Financial Risk Management footnote included as part of the Company's Audit Report as of October 31, 2020.

*Holding of User and Merchant Assets*

The Company holds both user and merchant cash and cryptocurrency balances. At this time the risk of any fluctuations in currency balances held for these parties is the sole risk of the user or merchant. The Company does not have a risk on the holding of these accounts for a currency risk fluctuation. The Company has the obligation of stewardship of both user and merchant accounts. Fiat funds reside within and behind the security protocols of a major Canadian Bank.

*Cybersecurity*

Cyberattacks and security breaches of our platform, or those impacting our customers or third parties, could adversely impact our brand and reputation and our business, operating results, and financial condition. Our business involves the collection, storage, processing, and transmission of confidential information, customer, employee, service provider, and other personal data, as well as information required to access customer assets. We have built our reputation on the premise that our platform offers customers a secure way to purchase, store, and transact in crypto assets. As a result, any actual or perceived security breach of us or our third-party partners may:

- harm our reputation and brand;
- result in our systems or services being unavailable and interrupt our operations;
- result in improper disclosure of data and violations of applicable privacy and other laws;

- result in significant regulatory scrutiny, investigations, fines, penalties, and other legal, regulatory, and financial exposure;
- cause us to incur significant remediation costs;
- lead to theft or irretrievable loss of our or our customers' fiat currencies or crypto assets;
- reduce customer confidence in, or decreased use of, our products and services;
- divert the attention of management from the operation of our business;
- result in significant compensation or contractual penalties from us to our customers or third parties as a result of losses to them or claims by them; and
- adversely affect our business and operating results.

Further, any actual or perceived breach or cybersecurity attack directed at other financial institutions or crypto companies, whether or not we are directly impacted, could lead to a general loss of customer confidence in crypto or in the use of technology to conduct financial transactions, which could negatively impact the Company, including the market perception of the effectiveness of our security measures and technology infrastructure.

An increasing number of organizations, including large merchants, businesses, technology companies, and financial institutions, as well as government institutions, have disclosed breaches of their information security systems, some of which have involved sophisticated and highly targeted attacks, including on their websites, mobile applications, and infrastructure.

Attacks upon systems across a variety of industries, including the cryptocurrency industry, are increasing in their frequency, persistence, and sophistication, and, in many cases, are being conducted by sophisticated, well-funded, and organized groups and individuals, including state actors. The techniques used to obtain unauthorized, improper, or illegal access to systems and information (including customers' personal data and crypto assets), disable or degrade services, or sabotage systems are constantly evolving, may be difficult to detect quickly, and often are not recognized or detected until after they have been launched against a target. These attacks may occur on our systems or those of our third-party service providers or partners. Certain types of cyberattacks could harm us even if our systems are left undisturbed. Additionally, certain threats are designed to remain dormant or undetectable until launched against a target and we may not be able to implement adequate preventative measures.

Although we have developed systems and processes designed to protect the data we manage, prevent data loss and other security breaches, effectively respond to known and potential risks, and expect to continue to expend significant resources to bolster these protections, there can be no assurance that these security measures will

provide absolute security or prevent breaches or attacks. We may experience in the future, breaches of our security measures due to human error, malfeasance, insider threats, system errors or vulnerabilities, or other irregularities. Unauthorized parties could attempt, and we expect that there are those who will continue to attempt, to gain access to our systems, as well as those of our customers, partners, and third-party service providers, through various means. Certain threat actors may be supported by significant financial and technological resources, making them even more sophisticated and difficult to detect. Further, there has been an increase in such activities as a result of the novel coronavirus, or COVID-19, pandemic. As a result, our costs, and the resources we devote to protecting against these advanced threats and their consequences may continue to increase over time.

The Company could be potentially exposed and may not have sufficient insurance to protect us against all losses and costs stemming from security breaches, cyberattacks, and other types of unlawful activity, or any resulting disruptions from such events. Outages and disruptions of our platform, including any caused by cyberattacks, may harm our reputation and our business, operating results, and financial condition.

*Operational Risks*

The success of the Company is dependent upon the ability, expertise, judgment, discretion, and good faith of its senior management. While employment agreements are customarily used as a primary method of retaining the services of key employees, these agreements cannot assure the continued services of such employees. Any loss of the services of such individuals could have a material adverse effect on our business, operating results, or financial condition.

*Risks Associated with Private Keys*

The loss or destruction of private keys required to access any crypto assets held in custody for our own account or for our customers may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to our ability to access any crypto assets, it could cause regulatory scrutiny, reputational harm, and other losses.

Crypto assets are generally controllable only by the possessor of the unique private key relating to the digital wallet in which the crypto assets are held. While blockchain protocols typically require public addresses to be published when used in a transaction, private keys must be safeguarded and kept private in order to prevent a third party from accessing the crypto assets held in such a wallet. To the extent that any of the private keys relating to our hot or cold wallets containing crypto assets held for our own account or for our customers is lost, destroyed, or otherwise compromised or unavailable, and no backup of the private key is accessible, we will be unable to access the crypto assets held in the related wallet. Further, we cannot provide assurance that our wallet will not be hacked or compromised. Crypto assets and blockchain technologies have been, and may in the future be, subject to security

breaches, hacking, or other malicious activities. Any loss of private keys relating to, or hack or other compromise of, digital wallets used to store our customer's crypto assets could adversely affect our customer's ability to access or sell their crypto assets, require us to reimburse our customers for their losses, and subject us to significant financial losses in addition to losing customer trust in us and our products. As such, any loss of private keys due to a hack, employee or service provider misconduct or error, or other compromise by third parties could hurt our brand and reputation, result in significant losses, and adversely impact our business. The total value of crypto assets in our possession and control is significantly greater than the total value of insurance coverage that would compensate the Company in the event of theft or other loss of funds.

*Pandemic Risks*

The Company cautions that current global uncertainty with respect to the spread of the COVID-19 virus ("COVID-19") and its effect on the broader global economy may have a significant negative effect on the Company. While the precise impact of COVID-19 on the Company remains unknown, rapid spread of the COVID-19 may have a material adverse effect on global economic activity, and can result in volatility and disruption to global supply chains, operations, mobility of people and the financial markets, which could affect interest rates, credit ratings, credit risk, inflation, business, financial conditions, results of operations and other factors relevant to the Company.

*Regulatory Environment*

Our business is or may become subject to extensive laws, rules, regulations, policies, orders, determinations, directives, treaties, and legal and regulatory interpretations and guidance in the markets in which we operate, including those governing financial services and banking, securities dealing and marketplaces, commodities, crypto asset custody, exchange, and transfer, cross-border and domestic money and crypto asset transmission, foreign currency exchange, privacy, data protection, payment services (including payment processing and settlement services), bankruptcy, tax, anti-bribery, economic and trade sanctions, anti-money laundering, and counter-terrorist financing. Many of these legal and regulatory regimes were adopted prior to the advent of the internet, mobile technologies, crypto assets, and related technologies. As a result, they do not contemplate or address unique issues associated with the crypto economy, are subject to significant uncertainty, and vary widely across Canadian and international jurisdictions. These legal and regulatory regimes, including the laws, rules, and regulations thereunder, evolve frequently and may be modified, interpreted, and applied in an inconsistent manner from one jurisdiction to another, and may conflict with one another. Moreover, the complexity and evolving nature of our business and the significant uncertainty surrounding the regulation of the crypto economy requires us to exercise our judgement as to whether certain laws, rules, and regulations apply to us, and it is possible that governmental bodies and regulators may disagree with our conclusions. To the extent we have not complied with such laws, rules, and regulations, we

could be subject to significant fines, revocation of licenses, limitations on our products and services, reputational harm, and other regulatory consequences, each of which may be significant and could adversely affect our business, operating results, and financial condition.

In addition to existing laws and regulations, various governmental and regulatory bodies, including legislative and executive bodies in Canada and in other countries may adopt new laws and regulations, or new interpretations of existing laws and regulations may be issued by such bodies or the judiciary, which may adversely impact our legal and regulatory status by changing how we operate our business, how our products and services are regulated, and what products or services our competitors and we can offer, requiring changes to our compliance and risk mitigation measures, imposing new licensing requirements, or imposing a total ban on certain crypto asset transactions, as has occurred in certain jurisdictions in the past.

On March 29, 2021, the Canadian Securities Administrators ("CSA") and the Investment Regulatory Organization of Canada ("IIROC") published Staff Notice 21-329 – Guidance for Crypto-Asset Trading Platforms ("CTPs"): Compliance with Regulatory Requirements ("Staff Notice 21-329") which provides guidance on how securities legislation applies to CTPs. Staff Notice 21-329 provides that CTPs that operate in a manner similar to crypto marketplace or are in the business of trading security tokens or crypto contracts will be required to seek registration as a dealer or marketplace or both. The Company is currently in dialogue with the BCSC regarding the application of Staff Notice 21-329 to the Company and its implications for the Company. The is no assurance that the Company will register as required by the CSA or if it does so, its application will be successful.

While we have implemented policies and procedures designed to help monitor for and ensure compliance with existing and new laws and regulations, however there can be no assurance that we and our employees, contractors, and agents will not violate or otherwise fail to comply with such laws and regulations. To the extent that we or our employees, contractors, or agents are deemed or alleged to have violated or failed to comply with any laws or regulations, including related interpretations, orders, determinations, directives, or guidance, we or they could be subject to civil, criminal, and administrative fines, penalties, orders and actions, including being required to suspend or terminate the offering of certain products and services, any of which outcomes could have a material adverse effect on the Company.

*Anti-Money Laundering (AML) – Know Your Customer (KYC)*

The Company has implemented internal proprietary AML/KYC protocols as well as utilizing third-party identification authentication to meet current regulations regarding this matter. Though regulation is extensive and designed to protect consumers and the public, its complex and sometimes ambiguous. The Company believes that it is in compliance with all current laws and regulations.

Reliance on Third Party Service Providers

We currently rely on third-party service providers for certain aspects of our operations, and any interruptions in services provided by these third parties may impair our ability to support our customers.

We rely on third parties in connection with many aspects of our business, including liquidity providers to convert cryptocurrency to fiat currency, banks to settle merchants and users; cloud computing services and data centers that provide facilities, infrastructure, website functionality and access, components, and services, including databases and data center facilities and cloud computing; third party KYC, compliance, risk, and intelligence platforms to validate users and transactions. Because we rely on third parties to provide these services and to facilitate certain business activities, we face increased operational risks. We do not control the operation of any of these third parties, including the data center facilities used. These third parties may be subject to financial, legal, regulatory, and labour issues, cybersecurity incidents, break-ins, computer viruses, denial-of-service attacks, sabotage, acts of vandalism, privacy breaches, service terminations, disruptions, interruptions, and other misconduct. They are also vulnerable to damage or interruption from human error, power loss, telecommunications failures, fires, floods, earthquakes, hurricanes, tornadoes, pandemics (including the COVID-19 pandemic) and similar events. In addition, these third parties may breach their agreements with us, disagree with our interpretation of contract terms or applicable laws and regulations, refuse to continue, or renew these agreements on commercially reasonable terms or at all, fail or refuse to process transactions or provide other services adequately, take actions that degrade the functionality of our services, impose additional costs or requirements on us or our customers, or give preferential treatment to competitors. There can be no assurance that third parties that provide services to us or to our customers on our behalf will continue to do so on acceptable terms, or at all. If any third parties do not adequately or appropriately provide their services or perform their responsibilities to us or our customers on our behalf, such as if third-party service providers close their data center facilities without adequate notice, or are unable to restore operations and data, or fail to perform as expected, or experience other unanticipated problems, we may be unable to procure alternatives in a timely and efficient manner and on acceptable terms, or at all, and we may be subject to business disruptions, losses or costs to remediate any of the deficiencies, customer dissatisfaction, reputational damage, legal or regulatory proceedings, or other adverse consequences which could harm our business.

In order to mitigate open-source risks, we track the open-source components that we are using, including all their dependencies, while keeping on top of information and updates coming from the open-source community. The best way to ensure we are one step ahead of the risks, without missing a beat, is to incorporate automated tools that continuously track our open-source usage and match them up against the most current data about open-source components, their vulnerabilities, risks, fixes and updates. Automated open-source management tools allow us to

put our ear on the pulse of the open-source community, and keep a constant eye on our open-source usage, helping us remain open-source risk-free.

*Custody and Safeguarding of Digital Assets*

All of the NetCents Technology cryptocurrency assets are held in a secure lockdown wallet server behind a multi layered firewall and restricted ACL along with Google Authenticator 2FA protection. Only the CTO and one senior developer have access to this server. Private keys are currently stored on the wallet service, which is secured by multi layered firewalls, restricted ACL, and Google Authenticator 2FA.

NetCents has migrated its cryptocurrency wallet system to a third-party Wallet as a Service provider. NetCents is a custodial wallet system that safeguards and maintains all private keys. The system monitors and maintains user transactions and facilitates deposit and withdrawal requests. User assets are held in various ways, including across multiple blockchain protocols. NetCents may transfer these assets from time to time to facilitate easy access to trading partners and to accommodate user requests. NetCents user accounts are not segregated. All assets of the company are fungible and replenished from time to time as needed. All user funds are liabilities of NetCents and are continuously monitored to maintain any user transactions or facilitate any requests for withdraws.

In order to mitigate cyber security risks, the company has implemented the following technical measures: DDOS protection, rate limiting, IP banning, in-house PEN testing, server monitoring, multi-layered and networked firewalls, IP restrictions and blacklisting, Google Authenticator 2FA, and continuous education and training for users on phishing emails and the various methods used to attack cryptocurrency wallets.

The frequency of monetization of cryptocurrency assets into fiat currency is rapid within the NetCents ecosystem. Nearly 99% of the volume on the merchant gateway uses the platforms' Instant Settlement technology meaning that the funds are changed from cryptocurrency to fiat as soon as the transaction is confirmed, and the fiat funds are paid out to the merchants' bank account. In the user portal and NC Exchange, approximately 2-3% of users hold their cryptocurrency funds in the platform. The remaining users remove the cryptocurrency to an external wallet once the cryptocurrency purchase has been completed. When fiat funds are loaded into the system by users, the funds are used to purchase cryptocurrency, on average, within week, and in most cases the cryptocurrency is then removed to an external wallet.

*Control Fundamentals*

The Company platform facilitates the movement of funds between parties, the storing of funds in a NetCents wallet and interaction with user and merchant bank accounts. To this end the Company has in place the following security protocols:

- The Platform protects the account holders from fraud and ID Theft. When using the platform, the consumer's bank account number/credit card numbers or any personal information are not transmitted over the Internet.
- No Transmission of Personal Data - When a transaction occurs, there is no personal ID or account information attached to the transaction. This lack of personal information prevents online fraud and ID theft.
- All customer data (personal and/or account related) remains protected and secure behind multiple firewall and encryption. Mail fraud is also eliminated as no paper statements are issued.
- The Company platform logs all transaction activity, and the system maintains a complete audit trail of all transactions, financial and otherwise.
- There is a daily reconciliation of all consumer and merchant activity is conducted at the close of each business day.
- The Company is also able to place thresholds on user's accounts so as to monitor transactions by type, location and volume so as to ensure compliance with applicable Know Your Customer (KYC), anti-money Laundering (AML), and anti-terrorism laws.
- Digital Authorization Required - Users are further protected as the Company cannot reach into a user's bank account. The user's account is a separate and secure entity to which the user deposits funds for payment. Additional funds cannot be removed from the user's account without the account holder's digital authorization.
- Payments made to a merchant after the completion of a transaction are fully automated, and the amount due is automatically generated by the system.
- The Company holds users and merchant funds in external exchanges and with a major Canadian and US Bank. The system and processes are required to safeguard these assets for both parties. To that end the Company has in place the following: multi-signature and two-party authorization for withdrawl of funds from the bank accounts and merchant funds held in an insured FBO/Trust account that is fully segregated from operating accounts.
- Mandatory Google Authenticator 2FA on all user withdrawals from the platform along with email notification of the withdrawal.
- Automated settlement via EFT network for all Canadian user withdrawals to eliminate human error.

**Cautionary Note Regarding Forward Looking Statements**

Forward-looking information is based upon estimates and assumptions of management in light of management's experience and perception of trends, current conditions and expected developments, as well as other factors that management believes to be relevant and reasonable in the circumstances, as of the date of this MD&A including, without limitation, assumptions about: favourable equity and debt capital markets; the ability to raise any necessary additional capital on reasonable terms to advance ; the Company's business plan; the timing and results of business developments; future currency exchange rates and interest rates; regulatory stability; the receipt of governmental, regulatory and third party approvals, licenses and permits on favourable terms; obtaining required renewals for existing approvals, licenses and permits on favourable terms; requirements under applicable laws; availability of equipment; and satisfying the terms and conditions of the Company's current loan arrangements. While the Company considers these assumptions to be reasonable, the assumptions are inherently subject to significant business, social, economic, political, regulatory, competitive and other risks and uncertainties, contingencies and other factors that could cause actual actions, events, conditions, results, performance or achievements to be materially different from those projected in the forward-looking information. Many assumptions are based on factors and events that are not within the control of the Company and there is no assurance they will prove to be correct.

Forward-looking information involves known and unknown risks, uncertainties and other factors, and do not guarantee future performance. Risks and uncertainties that may cause actual results or developments to be materially different from those expressed in forward-looking information.

Although the Company has attempted to identify important factors that could cause actual actions, events, conditions, results, performance or achievements to differ materially from those described in forward-looking information, there may be other factors that cause actions, events, conditions, results, performance or achievements to differ from those anticipated, estimated or intended. See "Risks and Uncertainties" for a discussion of certain risk factors investors should carefully consider before investing in the Company.

The Company cautions that the foregoing lists of important assumptions and factors are not exhaustive. Other events or circumstances could cause actual results to differ materially from those estimated or projected and expressed in, or implied by, the forward-looking information contained herein. There can be no assurance that forward-looking information will prove to be accurate, as actual results and future events could differ materially from those anticipated in such information. Accordingly, readers should not place undue reliance on forward-looking information.

Forward-looking information contained herein is made as of the date of this MD&A and the Company disclaims any obligation to update or revise any forward-looking information, whether as a result of new information, future events or results or otherwise, except as and to the extent required by applicable securities laws.