



Law Society
of Ontario

Barreau
de l'Ontario

Anti-Money Laundering: Protecting Your Litigation Practice

CO-CHAIRS

Gerald Chan
Stockwoods LLP

Lia Di Giulio, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

October 17, 2023



* C L E 2 3 - 0 1 0 0 6 0 1 - D - W E B *



Law Society
of Ontario

Barreau
de l'Ontario

CPD Materials Disclaimer & Copyright

These materials are part of the Law Society of Ontario's initiatives in Continuing Professional Development. Their content, including information and opinions, provided by the authors, is that of the authors. The content does not represent or embody any official position of, or statement by, the Law Society of Ontario, except where specifically indicated, nor should any content be understood as providing definitive practice standards or legal advice. The Law Society of Ontario does not warrant the current or future accuracy of the content and expressly disclaims responsibility for any errors and omissions in the content, including inaccuracies that may result due to developments in law.

Copyright in the materials is owned by the Law Society of Ontario. The content of the materials, including any graphic images, is protected by copyright both as individual works and as a compilation. No user of the materials may sell, republish, copy, reproduce, modify or distribute the materials or any portion thereof without the prior written permission of the Law Society of Ontario and other applicable copyright holder(s).

© 2023 All Rights Reserved

Law Society of Ontario

130 Queen Street West, Toronto, ON M5H 2N6
Phone: 416-947-3315 or 1-800-668-7380 Ext. 3315
Fax: 416-947-3370
E-mail: cpd@lso.ca
www.lso.ca

Library and Archives Canada
Cataloguing in Publication

Anti-Money Laundering: Protecting Your Litigation Practice

ISBN 978-1-77345-735-2 (PDF)



Anti-Money Laundering: Protecting Your Litigation Practice



CO-CHAIRS: **Gerald Chan**, *Stockwoods LLP*

Lia Di Giulio, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

October 17, 2023

9:00 a.m. to 12:15 p.m.

Total CPD Hours = 3 h + 15 m Professionalism ^P

**Law Society of Ontario
Donald Lamont Learning Centre
130 Queen St. W.
Toronto, ON**

SKU CLE23-01006

Agenda

9:00 a.m. – 9:10 a.m.

Welcome

Gerald Chan, *Stockwoods LLP*

Lia Di Giulio, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

9:10 a.m. – 9:55 a.m.

Cryptocurrency Considerations

Michael Fawcett, Crown Law Office – Criminal, *Ministry of the Attorney General*

Fredrick Schumann, *Stockwoods LLP*

Evan Thomas, *Wealthsimple Inc.*

9:55 a.m. – 10:10 a.m.

FINTRAC Guidance

Michael Boole, Manager – Anti-Money Laundering Unit, *Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)*

10:10 a.m. – 10:35 a.m.

Criminal Prosecutions

Benjamin Lerer, Crown Counsel, Serious Fraud Office, *Ministry of the Attorney General*

Lynda Morgan, *Addario Law Group LLP*

10:35 a.m. – 10:40 a.m.

Question and Answer Session

10:40 a.m. – 10:55 a.m.

Coffee and Networking Break

10:55 a.m. – 11:10 a.m.

Financial Institution Perspective

Paul Saguil, AVP, *TD Bank Group*

11:10 a.m. – 11:40 a.m.

Asset Forfeiture/Freezing

Melissa Adams, Crown Law Office – Criminal, *Ministry of the Attorney General*

Graeme Hamilton, *Borden Ladner Gervais LLP*

11:40 a.m. – 11:45 a.m.

Question and Answer Session

11:45 a.m. – 12:15 p.m.

Lawyers Ethical Obligations

Phil Brown, Acting Director, Practice Supports &
Resources, *Law Society of Ontario*

Gerald Chan, *Stockwoods LLP*

Lia Di Giulio, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

12:15 p.m.

Program Ends



This program qualifies for the 2025 LAWPRO Risk Management Credit

What is the LAWPRO Risk Management credit program?

The LAWPRO Risk Management Credit program pays you to participate in certain CPD programs. For every LAWPRO-approved program you take between September 16, 2023 and September 15, 2024, you will be entitled to a \$50 premium reduction on your **2025 insurance premium** (to a maximum of \$100 per lawyer). Completing any Homewood Health Member Assistance Plan e-learning course available at homeweb.ca/map also qualifies you for a \$50 credit.

Why has LAWPRO created the Risk Management Credit?

LAWPRO believes it is critical for lawyers to incorporate risk management strategies into their practices, and that the use of risk management tools and strategies will help reduce claims. Programs that include a risk management component and have been approved by LAWPRO are eligible for the credit.

How do I qualify for the LAWPRO Risk Management Credit?

Attendance at a qualifying CPD program will NOT automatically generate the LAWPRO Risk Management Credit. To receive the credit on your 2025 invoice, you must log in to [My LAWPRO](#) and completing the online Declaration Form in the Risk Management Credit section.

STEP 1:	STEP 2:
<ul style="list-style-type: none">• Attend an approved program in person or online; and/or• View a past approved program• Completing a Homewood Health e-course*	Complete the online declaration form in the Risk Management Credit section of my.lawpro.ca by September 15, 2024. The credit will automatically appear on your 2025 invoice.

You are eligible for the Risk Management Credit if you chair or speak at a qualifying program provided you attend the entire program.

Where can I access a list of qualifying programs?

See a list of current approved programs at lawpro.ca/RMcreditlist. Past approved programs are usually indicated as such in the program materials or download page. Free CPD programs offered by LAWPRO can be found at www.practicepro.ca/cpd

Whom do I contact for more information?

Contact practicePRO by e-mail: practicepro@lawpro.ca or call 416-598-5899 or 1-800-410-1013.

*One Homewood Health e-learning course is eligible for the credit on a yearly basis.



Anti-Money Laundering: Protecting Your Litigation Practice

October 17, 2023

SKU CLE23-01006

Table of Contents

TAB 1	<u>Cryptocurrency Considerations</u>
	Glossary of cryptocurrency terms.....1 - 1 to 1 - 3
	Fredrick Schumann, <i>Stockwoods LLP</i>
	Factum of the Applicant – Attorney General for Ontario1 - 4 to 1 - 45
	Alysa Holmes and Michael Fawcett, Crown Law Office – Criminal <i>Ministry of the Attorney General</i>
	Factum of <i>Amicus Curiae</i>.....1 - 46 to 1 - 88
	Michael W. Lacy and Bryan Badali, <i>Brauti Thorning LLP</i>
	Submitted by: Michael Fawcett, Crown Law Office – Criminal <i>Ministry of the Attorney General</i>
	Cryptocurrency Considerations (PowerPoint).....1 - 89 to 1 - 125
	Michael Fawcett, Crown Law Office – Criminal <i>Ministry of the Attorney General</i>

Fredrick Schumann, *Stockwoods LLP*

Evan Thomas, *Wealthsimple*

**TAB 2 FINTRAC Disclosures: Results through Financial
Intelligence (PowerPoint)2 - 1 to 2 - 1**

Michael Boole, Manager – Anti-Money Laundering Unit
*Financial Transactions and Reports Analysis Centre of
Canada (FINTRAC)*

**TAB 3 Money Laundering
Criminal Prosecutions (PowerPoint)3 - 1 to 3 - 22**

Benjamin Lerer, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

Lynda Morgan, *Addario Law Group LLP*

**TAB 4 Weblinks to Department of Finance Consultation Papers
and Stakeholder Submissions on Strengthening
Canada’s Anti-Money Laundering and
Anti-Terrorist Financing Regime4 - 1 to 4 - 2**

Paul Saguil, AVP, *TD Bank Group*

TAB 5 Asset Forfeiture/Freezing5 - 1 to 5 - 4

Melissa Adams, Crown Law Office – Criminal
Ministry of the Attorney General

Graeme Hamilton, *Borden Ladner Gervais LLP*

TAB 6	Law Society AML Resources	6 - 1 to 6 - 1
	8 Tips to Help Verify the Identity of an Individual	6 - 2 to 6 - 2

Phil Brown, Acting Director, Practice Supports & Resources
Law Society of Ontario



Law Society
of Ontario

Barreau
de l'Ontario

TAB 1

Anti-Money Laundering: Protecting Your Litigation Practice

Cryptocurrency Considerations

Glossary of cryptocurrency terms

Fredrick Schumann
Stockwoods LLP

October 17, 2023



Glossary of cryptocurrency terms

Fredrick Schumann, Stockwoods LLP

Address (or public key)	An alphanumeric identifier, akin to an account number or email address, that is used to store, receive, and send cryptocurrency.
Altcoin	Less popular cryptocurrencies. Sometimes the term is used to refer to any cryptocurrency other than Bitcoin.
Bitcoin (BTC)	The first, best-known, and most popular cryptocurrency.
Blockchain	A digital ledger existing in a distributed/decentralized database, maintained and updated simultaneously by multiple nodes on a network. Each cryptocurrency has its own blockchain showing all the transactions performed using that cryptocurrency.
Blockchain explorer	A blockchain explorer can be used to view the blockchain's data. For Bitcoin, www.blockchain.com can be used to view all transactions (amount sent, date and time, to and from what address).
Coin or token	A colloquial term for a cryptocurrency.
Cold wallet	A physical storage device such as a flash drive, hard drive or "solid state" drive used to store cryptocurrency offline. A Ledger device is a type of cold wallet.
Decentralized autonomous organization (DAO)	A DAO is an association where the relationship between the members of the association is governed by computer code. In a sense, a cryptocurrency is an example of a DAO. The Ethereum blockchain allows for more complex DAOs to be formed, using smart contracts to govern the relationship in a more sophisticated and flexible way.
DeFi (decentralized finance)	A way of conducting financial transactions and arrangements that does not rely on a centralized authority or intermediary. The Ethereum blockchain has evolved to offer a wide variety of financial services, such as lending facilities and investment products for digital assets. These services can be done using smart contracts on a peer-to-peer basis.
Ether	The native cryptocurrency of the Ethereum blockchain.
Ethereum	Another popular blockchain. Ethereum is more flexible than Bitcoin in that it is programmable. That means that routines and programs

	<p>that perform blockchain transactions, such as smart contracts and DeFi protocols, can be run on the Ethereum blockchain.</p> <p>Ether or ETH is the native cryptocurrency of the Ethereum blockchain.</p>
Fiat currency	Traditional modern currency, which is backed by a state or states.
Fork	A change to a blockchain's governing protocols. A fork can be a response to reverse a hack or other exploitation of a blockchain.
Gas	A per-transaction fee, in Ether, required to carry out transactions on the Ethereum blockchain.
Mining	In a proof-of-work system, the process of validating cryptocurrency transactions in exchange for a small amount of new cryptocurrency. Mining involves using high-powered computer systems to solve complex cryptography problems.
Mixer (or privacy mixer)	<p>A service designed to disguise the movement of tokens through a blockchain. Using a mixer breaks the link between the originating address and the recipient address, making it difficult for others to track the source of cryptocurrency in the recipient address. A user deposits cryptocurrency into the mixer's shared pool of cryptocurrency. The user then provides a secret direction to the mixer about where to send the same amount of cryptocurrency. The shared pool then sends out the cryptocurrency, but it is not the same cryptocurrency as was deposited by the user. Tornado Cash is an example of a privacy mixer.</p> <p>Also called a "tumbler."</p>
Monero	A privacy coin.
Non-fungible token (NFT)	A digital asset that is unique (i.e. non-fungible, unlike cryptocurrency) but that is transferred using blockchain technology (like cryptocurrency).
Peer-to-peer exchange	An online protocol that links sellers and buyers of cryptocurrency and facilitates exchanges between them.
Privacy coin	A cryptocurrency that is designed to maximize privacy.
Private key	A code akin to a password that is used to control a cryptocurrency address, including to carry out transactions.

Proof and work and proof-of-stake	<p>The two major consensus mechanisms underlying cryptocurrency. Proof-of-work (POW) is the older of the two, and it's used by Bitcoin, Ethereum, and others.</p> <p>In a POW blockchain, new transactions are added to the ledger as users ("miners") deploy powerful computer systems to race to solve cryptography problems. The first to solve the problem gets to update the ledger with the latest verified transactions. POW is an energy-intensive process, however.</p> <p>Proof-of-stake, or POS, is a newer alternative designed to meet the greater needs of more flexible blockchains such as Ethereum 2.0. In a POS blockchain, validators contribute or "stake" their own crypto in exchange for the change to validate a new transaction and update the blockchain. Successful validators receive a reward.</p>
Seed phrase	A set of words that can be used to recreate or recover a wallet.
Smart contract	A contract that executes itself by performing blockchain transactions, depending on certain conditions being met. In theory, two parties can make an agreement and reduce it to a smart contract that then performs or enforces itself without the parties needing to take any further action, and without the need to go to court if one party has not performed. A smart contract can be analogized to a vending machine, which performs the contract (dispensing the good) if a condition is met (the customer inserts the right amount of cash).
Stablecoin	A cryptocurrency that is designed to maintain value on par with a certain external measure of value, most commonly the US dollar.
Tumbler	Another term for a privacy mixer.
Wallet	<p>A protocol used to store private keys.</p> <p>Hot wallet: a wallet hosted by a custodian such as a cryptocurrency exchange or an application on a computer or mobile device. More convenient, but less secure from hacking.</p> <p>Cold wallet: a hardware device or even paper document that records the private keys. More secure, but less convenient and susceptible to loss or damage.</p>



Law Society
of Ontario

Barreau
de l'Ontario

TAB 1

Anti-Money Laundering: Protecting Your Litigation Practice

Cryptocurrency Considerations

Factum of the Applicant – Attorney General for Ontario

Alysa Holmes and Michael Fawcett, Crown Law Office – Criminal
Ministry of the Attorney General

October 17, 2023



SUPERIOR COURT OF JUSTICE
(Central East Region)

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

FACTUM OF THE APPLICANT

Ministry of the Attorney General
Crown Law Office – Criminal
720 Bay Street, 10th Floor
Toronto, Ontario, M7A 2S9

Alysa Holmes
Counsel for the Applicant
Tel: (437) 288-2793
Alysa.Holmes@ontario.ca

Michael Fawcett
Counsel for the Applicant
Tel: (416) 268-4342
Michael.Fawcett@ontario.ca

Table of Contents

PART I: INTRODUCTION.....	1
PART II: SUMMARY OF THE FACTS.....	2
A. Cryptocurrency: An overview.....	3
B. Cryptocurrency-related crime is on the rise	6
C. Cryptocurrency seizures.....	7
(1) The use of general warrants for cryptocurrency seizures.....	7
(2) The legal validity of the general warrant technique.....	10
D. The proposed digital asset amendments.....	12
E. The DRPS application	12
F. The application judge’s ruling.....	14
PART III: ISSUES AND THE LAW	15
A. The scope of <i>certiorari</i> review.....	15
(1) The caselaw	15
(2) Analysis.....	17
B. The application judge committed jurisdictional and legal error	19
(1) The seizure of proceeds.....	20
(2) The “no other provision” requirement	21
(3) The inadequate alternatives.....	23
C. This Court should exercise its discretion to grant <i>certiorari</i> with <i>mandamus</i>	29
(1) The remaining general warrant criteria are satisfied.....	29
(2) There is a national interest in confirming the validity of the general warrant technique	33
PART IV: ORDER REQUESTED	34
SCHEDULE A: AUTHORITIES TO BE CITED	35
Jurisprudence	35
Secondary Material: Government Documents.....	37
Secondary Material: Online Sources	37
SCHEDULE B: RELEVANT LEGISLATIVE PROVISIONS	39

PART I: INTRODUCTION

1. This application for *certiorari* with *mandamus* relates to the continued validity of a law enforcement technique that, today, is the **only** available tool for police to recover cryptocurrency that has been taken from Canadian victims *via* cybercrime by individuals outside the reach of our criminal justice system.
2. Every year, countless Canadians are tricked or forced into sending large sums of money, in the form of cryptocurrency, to online fraudsters and other cybercriminals located all over the globe. Although the crimes they commit are notorious and clear, these criminal actors are rarely – if ever – the subject of Canadian charges. These persons go unpunished and, year after year, the losses associated with online cryptocurrency-related crime continue to grow at a staggering rate.
3. Despite the recent proliferation of such crimes in Canada, Parliament has yet to enact clear, specific authority that expressly covers digital assets and permits law enforcement to seize stolen cryptocurrency that qualifies as proceeds of crime from the accounts of foreign cyber-criminals. As a result, it is the Attorney General for Ontario’s view that the residual seizure authority provided by the general warrant provision of the *Criminal Code* is the only existing legal mechanism capable of authorizing the police to carry out this vital state objective. To that end, in recent years, police agencies across Canada have used general warrants to seize significant sums of stolen or illegally obtained cryptocurrency, to be disposed of under the supervision of a Canadian court in accordance with law.
4. Today, this practice is in jeopardy. On March 7, 2023, the Durham Regional Police Service (“DRPS”) sought a general warrant and related assistance order to seize stolen cryptocurrency from addresses held at Binance Holdings Ltd. (“Binance”), the world’s largest cryptocurrency exchange. The application related to an investigation into alleged offences of fraud and possession of property obtained by crime arising out of an online cryptocurrency investment and romance scam committed against a Canadian victim. Binance is prepared to comply with the orders. There is no dispute that there are grounds to believe the offences occurred and the funds are proceeds. The suspects – whose accounts have been frozen for over a year – are three Nigerian citizens who have never once reached out to Canadian law enforcement to assert an interest in the property.

5. Still, the Honourable Justice Burstein of the Ontario Court of Justice in Oshawa (“the application judge”) rejected the application. He issued a published written decision explaining the result, stating that he refused to grant the general warrant on the basis that a general warrant could not “stretch” to cover the police objective. The judge questioned the police practice and appropriateness of using a general warrant to seize *digital* proceeds of crime.

6. The Attorney General for Ontario now applies for an order in the nature of *certiorari* with *mandamus* to quash the application judge’s order dismissing the DRPS application and to compel the Ontario Court of Justice to exercise its jurisdiction to issue the requested general warrant and related assistance order. In the applicant’s respectful view, the judge committed jurisdictional and legal errors that justify the requested relief. There is no question the police can use a traditional *Criminal Code* investigative tool (like a search warrant) to seize stolen property (like cash or a diamond ring) for later disposition pursuant to the comprehensive regime set out in the *Code*. Cryptocurrency is just another form of stolen property, and its seizure ought to be no different.

PART II: SUMMARY OF THE FACTS

7. The following paragraphs refer to some factual material (*e.g.*, information on cybercrime, cryptocurrency, and previous general warrant applications) that were not discussed in the original Information to Obtain (“ITO”). These sections have been included to provide what the Crown believes is important background information on the relevant legal landscape, and to situate the application judge’s decision in context and underscore its significance.

8. The applicable case law supports this approach. As a general matter, courts have accepted that a *certiorari* applicant can supplement the record with background facts.¹

9. The rule makes sense. It remains open to DRPS to file an entirely new application for the same general warrant before either this Court or the lower court – on either the same or an entirely new evidentiary record – so long as it discloses the prior rejection.² In the applicant’s view, there

¹ See *e.g.* *R. v. Domstad*, [2001 ABQB 179](#) at para. 39 (“It may be that a record under scrutiny on a motion for *certiorari* and prohibition can be supplemented by evidence going to the competence or legality of the court itself”); *Re Section 487.02 of the Criminal Code*, [2019 NLCA 6](#) at paras. 16-20; *R. v. Blais*, [2008 BCCA 389](#) at para. 7; *Ward v. University of Prince Edward Island*, [1997 CanLII 4643](#) (PE SCTD) at para. 21.

² See *R. v. Bond*, [2021 ONCA 730](#) at paras. 22-35; *R. v. Colbourne* (2001) [157 C.C.C. \(3d\) 273](#) at paras. 40-42 (Ont. C.A.); *R. v. Stewart*, [2017 ONSC 7193](#) at para. 35; *R. v. Persaud*, [2016 ONSC 8110](#) at paras. 113-19; *R. v. Campbell*, [\[2014\] O.J. No. 6541](#) at paras. 56-58 (Sup. Ct.); *R. v. Comtois*, [2017 QCCA 1376](#) at para. 22; *R. v. Duchcherer*, [2006 BCCA 171](#) at paras. 13-38.

is no substantive difference between supplementing the record here, on an application for *certiorari*, and filing a fresh application (with additional facts) for the same general warrant. In fact, the standard of review faced by the applicant on a petition for *certiorari* is arguably *narrower* than the one that would apply on a *de novo* application, as discussed below.

A. Cryptocurrency: An overview

10. Cryptocurrency is a relatively new concept for the Canadian legal system and Canadian law enforcement. The applicant thus starts with an overview of several key cryptocurrency concepts. These concepts are also explained in depth in the ITO, which includes a comprehensive set of definitions.³

11. Cryptocurrency is a digital asset. Like other assets – for example, real estate or a commodity like gold – it can be bought, sold, traded, and exchanged. There are thousands of different types of cryptocurrencies. The cryptocurrency at issue in this case – called Bitcoin – is the world’s first and most popular cryptocurrency. Unlike fiat currency, which corresponds to physical or traditional money, cryptocurrency exists purely as digital entries to an online database or ledger, called the “blockchain.” The blockchain is simply a new word for a familiar concept. It is an online ledger that, just like any other financial ledger, can track every transaction for a given asset (e.g., Bitcoin).⁴

12. The Bitcoin blockchain is public. That is important, because it means anyone can go online and view the details of any Bitcoin transaction that has ever occurred. This function theoretically allows anyone, including the police, to trace cryptocurrency transactions from point to point (or “address” to “address,” a term discussed below). However, despite being public, the Bitcoin blockchain is also designed to maintain a level of *anonymity*. This is because, while all the transactions are public, they are not linked to the names of the persons transferring the funds. Users employ a system of “public” and “private” keys to send, receive, and store cryptocurrency.⁵

³ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 18-23.

⁴ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 18-19. See also Supplemental Affidavit of Taryn Snow at para. 23; Ontario Securities Commission, “[Crypto 101: Glossary](#)”.

⁵ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 19-20. See also Supplemental Affidavit of Taryn Snow at paras. 23-24; Ontario Securities Commission, “[Crypto 101: Glossary](#)”.

13. The system works as follows. The public key is a series of alphanumeric characters used to receive cryptocurrency. Public keys are very long, so a shorter, related “public address” is typically generated in order to facilitate the transfer of funds. A public address is intended to be made public. It functions like a bank account or e-mail address or P.O. Box number. Just like you ask others to send an e-transfer to your e-mail address, you can provide someone with your public address and ask them to send you cryptocurrency. The *private key* is linked to your public address and allows you to access and control your funds. It functions like your PIN number or password or the physical key to your safety deposit box. The person who possesses the private key controls the cryptocurrency associated with the corresponding public address.⁶

14. An analogy helps illustrate how the system works in practice. Cryptocurrency transactions are like a bunch of people in a room, transferring assets or exchanging property, in public, on video. All of the transactions are recorded, on a public ledger or “blockchain”, for anyone to see. Except, the individuals in the room are all wearing masks or disguises. You can see what is happening, but it is not obvious who is involved.⁷

15. Usually, a transfer of cryptocurrency involves transferring the control of funds from the sender’s public address to the recipient’s public address, which the recipient can then access with their corresponding private key. The recipient now controls the funds. This transfer is recorded in the blockchain ledger, referencing the date, time, amount, to and from addresses, and other transactional details. The blockchain tells the world that the recipient’s public address now has ownership of the particular unit of cryptocurrency transferred.⁸

16. As noted above, this system is *generally* anonymous. But there is a vulnerability in that feature of the design.⁹ Cryptocurrency users often wish to convert their digital assets into fiat currency (*e.g.*, traditional cash). Doing so creates opportunities for onlookers to see who is involved in purchasing and selling the cryptocurrency.

17. For example, a cryptocurrency user may convert their digital assets into fiat currency using a cryptocurrency exchange, such as FTX, Binance, or Coinbase. A “cryptocurrency exchange” is

⁶ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 20-21. See also Supplemental Affidavit of Taryn Snow at para. 24.

⁷ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 19-20.

⁸ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 20-21. See also Supplemental Affidavit of Taryn Snow at para. 25.

⁹ See Wired, “[Cryptocurrency’s Myth of Anonymity](#)” (Feb. 9, 2023).

an online marketplace that operates like a brokerage, acting as an intermediary between buyers and sellers of cryptocurrency. Most cryptocurrency exchanges provide their users with an online “wallet” that stores the information required to control the user’s cryptocurrency, *i.e.*, the public and private key.¹⁰ The exchange may hold on to the private key, however, keeping exclusive control over its clients’ cryptocurrency for itself. It also may sweep and pool customer assets into large exchange-controlled addresses that contain a significant amount of funds.¹¹

18. Like most large financial institutions, cryptocurrency exchanges are required by law to keep detailed records about their clients.¹² And so, when law enforcement analyzes the public blockchain and sees illicit cryptocurrency move into a public address associated with a cryptocurrency exchange,¹³ the police can serve the exchange with a production order to de-anonymize the recipient of the proceeds.¹⁴

19. As discussed below, some cryptocurrency exchanges also will respond to Canadian court orders and transfer cryptocurrency from an exchange-controlled address into a police-controlled one.¹⁵ To give the police control over the alleged proceeds, the exchange simply uses the private key that controls cryptocurrency held in an exchange-controlled address, to send the amount of cryptocurrency specified in the court order to a new public address – one controlled by the police. The police can then use the private key associated with their public address to access and control the transferred cryptocurrency. This takes the funds out of the exchange’s control and puts them into police control. This transfer of ownership and control from the exchange-controlled address to the police-controlled address is recorded in the public blockchain.¹⁶

¹⁰ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 21-22. See also Supplemental Affidavit of Taryn Snow at para. 26.

¹¹ See Supplemental Affidavit of Taryn Snow at para. 26.

¹² See Osler, “[Anti-Money Laundering Rules for Cryptocurrency dealers finalized by Canadian Government](#)” (July 12, 2019) (noting that the Canadian Department of Finance had published amendments to the *PCMLTFA 2019* clarifying that virtual asset service providers are deemed to be Money Services Businesses and thus subject to FINTRAC reporting and the similar due diligence, reporting, monitoring, and reporting requirements as all other reporting entities). See also Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 24-25.

¹³ The ITO sets out how law enforcement can “trace” the flow of illegal funds and “attribute” addresses to cryptocurrency exchanges. See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 22-23, 34-38.

¹⁴ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 21-26, 46-47.

¹⁵ See e.g. Supplemental Affidavit of Taryn Snow at paras. 13(b), 19(a), (g).

¹⁶ See Affidavit of Taryn Snow at para. 26. See also Affidavit of Taryn Snow, Exhibit A: ITO, at p. 20.

B. Cryptocurrency-related crime is on the rise

20. Cybercrime has exploded as the world moves online. Our most intimate information is stored in the “cloud.”¹⁷ Our critical infrastructures are dependent upon well-functioning technology. Our financial security is tied to our online lives. Cybercrime now targets each of these modern paradigms and more.¹⁸ Ransomware attacks, data breaches, darknet marketplaces, and phishing emails have become all too commonplace. There are countless high-profile examples of recent cyberattacks that have profoundly impacted the daily lives of Canadians.¹⁹

21. The proliferation of cybercrime has been accompanied by a corresponding increase in the use of cryptocurrency to facilitate and profit from online crime.²⁰ For example: cryptocurrency has consistently been the second most common form for proceeds of fraud since 2018.²¹ The losses associated with these offences are substantial. In 2021 alone, the Canadian Anti-Fraud Centre counted them at \$75 million.²² Cryptocurrency is also the preferred method of payment in ransomware attacks, which generates billions of dollars in losses to Canadians each year – with the average ransom demand in the hundreds of thousands.²³

22. Despite the prevalence of cybercrime in Canada, cyber criminals frequently go unpunished due to the unique challenges associated with investigating and prosecuting these offences.²⁴ The reasons why are complicated. But one important component is that cyber threats are constantly evolving and – unlike traditional forms of crime – do not occur within easily defined territorial boundaries. Evidence of these offences is transient in nature and frequently spread across multiple

¹⁷ See *R. v. Vu*, [2013] 3 S.C.R. 657 at para. 44.

¹⁸ Canadian Centre for Cyber Security, “[National Cyber Threat Assessment, 2023-2024](#)”, at pp. iv-4. See also Supplemental Affidavit of Taryn Snow at para. 7.

¹⁹ See e.g. Emma McPhee, “[Gone Phishing: Cyber crime on rise in Canada, and it’s proving costly](#)”, *Postmedia News* (1 March 2023); Lee Berthiaume, “[Cyber attack hits engineering giant with contracts for military bases, power plants](#)”, *The Canadian Press* (8 March 2023); Ryan Tumilty, “[This could be the worst year ever for ransomware attacks: experts](#)”, *The National Post* (1 February 2023). See also Supplemental Affidavit of Taryn Snow at para. 7.

²⁰ See Supplemental Affidavit of Taryn Snow at para. 8.

²¹ Canadian Centre for Cyber Security, “[National Cyber Threat Assessment, 2023-2024](#)”, at pp. 6-7, 20; Canadian Anti-Fraud Centre, “[Annual Report: 2021](#)”, at pp. 3, 10-12. See also Supplemental Affidavit of Taryn Snow at para. 8.

²² Paul Northcott, “[Countering the rise of cryptocurrency fraud](#)”, *RCMP Gazette* (23 March 2022).

²³ Canadian Centre for Cyber Security, “[National Cyber Threat Assessment, 2023-2024](#)”, at pp. 6-7; “[Report: The cost of ransomware in 2020. A country-by-country analysis](#)”, *Emisoft Malware Labs* (11 February 2020) (Blog); Jade Markus, “[Reported ransomware attacks in Calgary dropped 41% last year](#)”, *CBC News* (11 February 2023). See also Supplemental Affidavit of Taryn Snow at para. 8.

²⁴ Affidavit of Taryn Snow, Exhibit A: ITO, at p. 52; See also Supplemental Affidavit of Taryn Snow at paras. 9-10; Financial Post, “[Safety Net: Crypto scams are duping thousands of Canadians, leaving them despondent and broke](#)” (March 9, 2023).

countries. And the cyber environment, coupled with the decentralized and global nature of cryptocurrency, has increasingly allowed foreign criminal actors to profit off Canadian victims while remaining beyond the reach of the Canadian justice system.²⁵

C. Cryptocurrency seizures

23. Cryptocurrency seizures are a recent development within the Canadian justice system. A summary of the state of the law surrounding cryptocurrency seizures and the use of general warrants for this purpose is set out below.

(1) The use of general warrants for cryptocurrency seizures

24. There is no clear legal mechanism in the *Criminal Code* permitting the police to seize stolen digital assets, such as cryptocurrency, and return them to their lawful owners.²⁶ As discussed below, the traditional search and proceeds of crime provisions were passed well before the rise of cryptocurrency and do not reference digital assets.

25. As such, Canadian police agencies have, as a general matter, turned to general warrants under s. 487.01 of the *Code* to fill this legislative gap.²⁷ Section 487.01 was enacted as a “legislative failsafe” aimed at filling potential gaps in the existing investigative powers in the *Code*. It provides judicial authorization for a broad and flexible range of investigative techniques or procedures in circumstances in which no other authority exists.²⁸

26. Canadian police have used general warrants to seize cryptocurrency in a variety of circumstances. The following lists are not intended to be exhaustive but rather a representation of what has occurred. Broadly speaking, general warrants have been used to carry out two different types of cryptocurrency seizures. The first relates to situations in which law enforcement seize a physical cryptocurrency wallet device – or the means of accessing cryptocurrency associated to a

²⁵ Canadian Anti-Fraud Centre, “[Annual Report: 2021](#)”, at pp. 7, 24; RCMP, “[RCMP Cybercrime Strategy](#)” (December 2, 2015), at pp. 6, 9; See also Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97; Supplemental Affidavit of Taryn Snow at para. 10.

²⁶ See Government of Canada, [Budget 2023](#), Ch. 5 (noting that the federal government is just now considering legislative changes that will “[g]ive law enforcement the ability to freeze and seize virtual assets with suspected links to crime”).

²⁷ See Supplemental Affidavit of Taryn Snow at paras. 11, 13, 19.

²⁸ *R. v. TELUS Communications Co.*, [2013 SCC 16](#) at para. 91 (Moldaver J.A., concur.) (“[G]eneral warrants were created to fill any potential ‘gap’, to provide a legislative ‘failsafe’ that supplement[s] rather than supplant[s], to ‘fill an investigatory hiatus’, and to serve as a ‘residual power’.” (citations and internal quotation marks omitted)). See also *R. v. Ha*, [2009 ONCA 340](#) at para. 35.

suspect wallet (*e.g.*, a private key) – during the search of a target location pursuant to a standard s. 487 search warrant. Upon finding the means to control the cryptocurrency, the police then seek a general warrant to transfer the funds to a police-controlled address.²⁹ For example:

- In 2021, the RCMP used a general warrant in the Netwalker ransomware investigation to seize approximately \$23 million in cryptocurrency from devices belonging to a ransomware hacker located in Gatineau who received ransom payments from his victims in cryptocurrency.³⁰
- In 2021, the RCMP seized approximately 0.15 Bitcoin³¹ from a fraud suspect’s cellphone pursuant to a general warrant. The seized cryptocurrency was forfeited following the suspect’s guilty plea and ultimately formed part of a restitution order.³²
- In 2021, the RCMP and Hamilton Police Service used a general warrant to seize about \$26,000 in cryptocurrency from a device located during the execution of a CDSA warrant.³³
- The OPP executed two general warrants authorizing cryptocurrency seizures between 2021 and 2022. In Project CODA, the OPP used a general warrant to seize cryptocurrency. In Project Archie, the OPP used a general warrant to seize about \$400,000 in cryptocurrency from a suspect’s cryptocurrency wallet during a firearms investigation. Both projects resulted in charges and remain before the courts.³⁴
- In 2022, the Newfoundland RCMP executed a general warrant to seize cryptocurrency from a suspect’s cryptocurrency wallet. The RCMP ultimately chose not to proceed with the seizure, as the target wallet only contained \$3 at the time of warrant execution.³⁵

²⁹ See *e.g.* Supplemental Affidavit of Taryn Snow at paras. 13, 19.

³⁰ *R. v. Vachon-Desjardins*, [2022 ONCJ 43](#) at paras. 7, 14 & n.4. See also Supplemental Affidavit of Taryn Snow at para. 13(a); “[The Fifth Estate: Hunting the Hacker of Gatineau](#)”, *CBC News* (7 November 2022).

³¹ The Crown calculates 0.15 BTC to have an approximate value of \$6340 based on the value Bitcoin as of June 30, 2021.

³² See Supplemental Affidavit of Taryn Snow at para. 19(b).

³³ See Supplemental Affidavit of Taryn Snow at para. 19(c).

³⁴ See Supplemental Affidavit of Taryn Snow at para. 19(d).

³⁵ See Supplemental Affidavit of Taryn Snow at para. 19(f).

- In 2022, the OPP seized hundreds of thousands of dollars in cryptocurrency from one of the organizers of the “Freedom Convoy” under the authority of a general warrant.³⁶ The seized cryptocurrency was ultimately turned over by the police to the escrow agent appointed in connection with ongoing civil proceedings.³⁷
- In 2023, the RCMP used a general warrant to seize over \$130,000 in various cryptocurrencies from three suspect cryptocurrency wallets identified as part of a drug trafficking investigation.³⁸

27. General warrants have also been used to seize stolen or illicitly obtained cryptocurrency proceeds in a second way, *i.e.*, from suspect wallets held by third-party cryptocurrency exchanges. This is the specific technique at issue in the instant application. Recent examples of this type of seizure include:

- In 2021, the DRPS used a general warrant to seize \$55,000 in stolen cryptocurrency from a target address held on the Binance exchange.³⁹
- In 2021 and 2022, the Toronto Police Service used general warrants to seize cryptocurrency from target addresses on the Binance exchange in four separate fraud or theft investigations. The total assets seized across all four investigations was over \$90,000.⁴⁰
- In 2022, the OPP seized an undisclosed sum of cryptocurrency from addresses on the Binance exchange in relation to the Freedom Convoy investigation.⁴¹
- In 2022, the Nova Scotia RCMP used general warrants to seize cryptocurrency from target addresses on the Binance exchange in two separate investigations. The first warrant was successfully used to seize the target cryptocurrency and transfer the funds to an RCMP

³⁶ See Supplemental Affidavit of Taryn Snow at para. 13(b). See also David Fraser, “[Digital currency donations for Freedom Convoy evading seizure by authorities](#)”, *CBC Investigates* (21 March 2022).

³⁷ See Supplemental Affidavit of Taryn Snow at para. 13(b). See also Financial Post, “[Police have turned crypto seized from trucker convoy over to escrow agent, court told](#)” (9 March 2022).

³⁸ See Supplemental Affidavit of Taryn Snow at para. 19(e).

³⁹ See Supplemental Affidavit of Taryn Snow at para. 12]. See also Paul Northcott, “[Police help victim of crypto-fraud get money back](#)”, *RCMP Gazette* (10 May 2022).

⁴⁰ See Supplemental Affidavit of Taryn Snow at para. 19(a).

⁴¹ See Supplemental Affidavit of Taryn Snow at para. 13(b).

controlled address. The RCMP chose not to execute the second warrant after discovering that the target funds could not be adequately linked to the victim.⁴²

28. In each one of these examples, the warrants were issued by a judge without written reasons. However, at least one judge has appeared to endorse the use of a general warrant for this type of cryptocurrency seizure. On April 11, 2023, the Honorable Justice Tchir of the Alberta Provincial Court found that a traditional s. 487 warrant to search a “building, receptacle, or place” was the incorrect warrant to seize cryptocurrency from addresses associated to a capital market company and instead identified a s. 487.01 general warrant as an alternative (citing several sources). The court also addressed the decision on review in the present matter and stated that the Honourable Justice Burstein’s ruling “doesn’t stand for the general proposition that a general warrant is inappropriate for seizing cryptocurrency.”⁴³

(2) The legal validity of the general warrant technique

29. The legal validity of using general warrants to seize cryptocurrency far from settled, however. In addition to the successful applications noted above, the applicant also is aware of recent decisions from courts in other provinces that have rejected general warrant applications for reasons similar to those identified by the application judge here.⁴⁴ Specifically:

- On February 14, 2023, the Honourable Justice Robertson of the Alberta Provincial Court rejected an application for a general warrant authorizing police to seize cryptocurrency from an exchange wallet for the express purpose of returning the funds to the victim. The judge concluded that general warrants are not intended to be used to return property lost due to an alleged offence.⁴⁵
- On April 14, 2023, the Honourable Justice Mulder of the B.C. Provincial Court rejected an application for a general warrant to seize cryptocurrency and “hold it in secure storage”.

⁴² See Supplemental Affidavit of Taryn Snow at para. 19(g).

⁴³ See Supplemental Affidavit of Taryn Snow at para. 21; Supplemental Affidavit of Taryn Snow, Exhibit B: Endorsement of Justice L.C. Tchir.

⁴⁴ See Supplemental Affidavit of Taryn Snow at para. 20.

⁴⁵ See Supplemental Affidavit of Taryn Snow, Exhibit A: Endorsement of Justice L.W. Robertson.

The judge found that the police failed to establish how the requested technique would provide information concerning the offence.⁴⁶

- On April 24, 2023, the Honourable Justice Lenehen of the Nova Scotia Provincial Court denied a general warrant application to seize cryptocurrency from an exchange wallet on the basis that the warrant would be unenforceable on an exchange without a physical or virtual presence in Canada. The judge did not address whether the general warrant criteria were otherwise satisfied.⁴⁷
- On June 2, 2023, the Honourable Justice Choy of the Provincial Court of Manitoba denied an application for a general warrant to seize cryptocurrency because, in the judge’s view, a restraint order was an adequate alternative mechanism of accomplishing the police objective of “recover[ing] proceeds of crime funds and return[ing] them to the lawful owner.” Also, the judge stated that “the unilateral seizing of intangible property from one individual and transferring it to another” on an *ex parte* application is not in the best interests of the administration of justice.⁴⁸

30. As set out in greater detail below, it is the Attorney General for Ontario’s respectful view that, for various reasons, these contrary decisions (1) misapprehend the proposed technique (*e.g.*, the police objective here is **not** simply to seize the suspects’ funds and return them to the victims *via* an *ex parte* procedure but rather to subject them to the clear *inter partes* disposition regime set out in the *Code*); (2) fail to appreciate that information is in fact conveyed to the police through the use of the technique; and (3) do not appreciate the limitations of the proceeds of crime restraint process, which makes it inappropriate for carrying out cryptocurrency seizures.

31. Nevertheless, the split of authority demonstrates the importance of the present application. There are decisions on the issue going both ways. And now, the application judge’s ruling is, to the Attorney General for Ontario’s knowledge, the only **published** decision about the validity of the technique. It is reasonable to believe that it will factor heavily in any future application concerning an attempted seizure of cryptocurrency proceeds.

⁴⁶ See Supplemental Affidavit of Taryn Snow, Exhibit A: Endorsement of Justice S. Mulder.

⁴⁷ See Supplemental Affidavit of Taryn Snow, Exhibit A: Endorsement of Justice G.E. Lenehen.

⁴⁸ See Supplemental Affidavit of Taryn Snow, Exhibit A: Endorsement of Justice L. Choy.

D. The proposed digital asset amendments

32. The legislative gap *vis-à-vis* digital assets has not gone without notice. To the contrary, Parliament has identified and taken steps toward remedying the problem. In the 2023 Federal Budget, the government stated its intention to introduce legislative amendments giving “law enforcement the ability to freeze and seize virtual assets with suspected links to crime”.⁴⁹ It followed this statement by proposing *Criminal Code* amendments addressing the seizure, management, and disposal of digital assets in the House of Commons on April 20, 2023. The provisions are currently under consideration by the Standing Committee on Finance. The proposed amendments include, *inter alia.*, the creation of a special warrant power permitting police to seize digital assets that constitute proceeds of crime.⁵⁰

33. However, as discussed in more detail below, the applicant respectfully submits that the proposed amendments are **not** a solution to the cryptocurrency seizure problem at the centre of this application. The availability of general warrants for cryptocurrency seizures will remain a critically important question even **if** the proposed digital asset amendments are passed.

E. The DRPS application

34. On March 7, 2023, Constable Taryn Snow of the DRPS (“the affiant”) applied to the Ontario Court of Justice in Oshawa for a s. 487.01 general warrant and a s. 487.02 assistance order to facilitate a seizure of cryptocurrency. The applications relate to an ongoing DRPS investigation into offences arising out of a cryptocurrency investment scam.⁵¹

35. There is no dispute that the ITO sets out sufficient grounds for believing that the alleged offences of fraud and possession of the proceeds of crime occurred, and that the targeted cryptocurrency constitutes the proceeds of those offences.⁵² In the Fall 2021, an unknown person(s) tricked the complainant into purchasing and transferring around \$65,000 worth of Bitcoin to wallet addresses outside the victim’s control. The DRPS traced a fraction of the complainant’s cryptocurrency – around 0.08 Bitcoin – to three wallet addresses (“the target

⁴⁹ Government of Canada, [Budget 2023](#), Ch. 5.

⁵⁰ See Bill C-57, [Budget Implementation Act](#), 2023, No. 1, 1st Sess, 44th Parl, 2023, ss. 212-227; Parliament of Canada, [Bill C-57](#).

⁵¹ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 15-16.

⁵² Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97-98. See also Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 47-49.

addresses”) held on the Binance exchange.⁵³ On May 30, 2023, this fraction was worth around \$3000 CAD.

36. The suspects in the investigation – who are currently in possession of the stolen cryptocurrency – are unlikely to face prosecution in Canada for the alleged offences. A production order served upon Binance confirmed that all three suspects are citizens of Nigeria who provided Nigerian places of residence.⁵⁴ Canada does not have an extradition treaty with Nigeria.⁵⁵

37. The DRPS sought to seize the subject cryptocurrency *via* a general warrant. Importantly, the stated goal of the general warrant was *not* simply to return the subject funds to the victim. Instead, the affiant was clear that the goal was to pause the movement of the proceeds; bring the funds under police control; and then let the criminal justice system determine the lawful owner pursuant to the process set out in the *Code*. The affiant identified this procedure as an “important investigative step” that would “assist in gathering information” about the alleged offences.⁵⁶

38. The affiant also stated her belief that there was “no other provision” capable of authorizing this procedure. She explained her view that all other potential options set out in the *Criminal Code* – including the restraint and management order provisions – are not an appropriate substitute for seizing cryptocurrency pursuant to a general warrant.⁵⁷

39. Finally, the affiant stated her belief that the proposed general warrant was in the best interests of the administration of justice, to the extent that it would “frustrat[e] the objective of the alleged fraud (*i.e.*, profiting off the unwitting and unsophisticated complainant)” and “assist in gathering information of the criminal offence.” The affiant further emphasized that cyber-related offences are “under-reported and under-investigated, and often go without punishment. But here, there is something that the police can do to respond to the fraud committed against the complainant.” The affiant felt she had “a responsibility to seize [the proceeds] if doing so would further the investigation of the offence.”⁵⁸

⁵³ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 35-38, 47-49.

⁵⁴ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97. See also Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 45-46.

⁵⁵ See Government of Canada, [Treaties](#).

⁵⁶ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 16, 51-52.

⁵⁷ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 49-52.

⁵⁸ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 51-52.

F. The application judge's ruling

40. The application judge dismissed the general warrant application. He accepted that there were reasonable grounds to believe the offence of fraud was committed; that this offence involved “the transmission of cryptocurrency from the victim to the suspects through the . . . exchange”; and that at least some of the stolen cryptocurrency “remains in the possession or control of the targeted exchange company on behalf of the suspects.” He also accepted that the cryptocurrency remaining in the target addresses was “probably ‘proceeds of crime’”.⁵⁹

41. The application judge recognized the difficulties associated with policing crimes involving cryptocurrency since these offences “typically involv[e] transnational entities and foreign suspects”. He commended DRPS for the “ingenuity” of seeking a general warrant in the circumstances.⁶⁰ He nevertheless refused to grant the general warrant for three reasons. All of them arise out of the judge’s view that the police were involved in impermissible asset recovery.

42. **First**, the application judge held that the general warrant requirement there be “no other provision” authorizing the technique or procedure was not met. He found that (1) the general warrant was “aimed at recovering property obtained by the commission of the offence” for the “sole purpose” of “future victim compensation”; and (2) there are “a variety of legal mechanisms” – including a s. 462.33 restraint order – that would have “authoriz[ed] an equivalent *interim* remedy”.⁶¹ (As discussed below, the applicant respectfully submits that this reasoning misapprehends the objective of the application and the abilities of a restraint order.) Regardless, the judge also concluded that even *if* there is “no other provision” authorizing the technique, the appropriate remedy is for Parliament to address the problem, not the courts.⁶²

43. **Second**, the application judge was not satisfied “that it would be legally appropriate to seek a general warrant for the purpose of seizing suspected proceeds of crime.” He emphasized that a general warrant may be authorized to obtain “information concerning the offence” and concluded that seizing property for “the sole purpose of future [victim] compensation” fell outside the scope of the provision.⁶³ Notably, the judge did not discuss whether the technique would provide

⁵⁹ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97.

⁶⁰ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97.

⁶¹ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-99.

⁶² Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-100.

⁶³ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-99.

information about the alleged possession of proceeds offence. His analysis on this point focussed exclusively on the alleged fraud.

44. **Third**, the application judge cautioned that using a general warrant in this manner was a potential abuse of process. His abuse concerns arose, in part, from his finding that the application failed to establish that the targeted cryptocurrency was the same cryptocurrency transferred by the victim. (As discussed below, this concern is grounded in a misapprehension of the cryptocurrency tracing explained in the ITO.) But perhaps more importantly, the judge viewed the application as an “unlawful” attempt to compensate the victim using the suspects’ money.⁶⁴

PART III: ISSUES AND THE LAW

A. The scope of *certiorari* review

45. There is an antecedent question as to whether the Crown is even entitled to seek *certiorari* with *mandamus* from a refusal by a provincial court judge to grant a general warrant.⁶⁵

(1) *The caselaw*

46. The applicant is not aware of any *certiorari* applications in respect of a refusal of a general warrant to seize cryptocurrency. However, Ontario courts have confirmed that an Attorney General may properly seek *certiorari* and *mandamus* in relation to decisions concerning similar *Criminal Code* investigative tools, such as search warrants and production orders.⁶⁶ The applicant sees no reason to distinguish the review rights arising out of a refusal of a general warrant from the legal options available upon the refusal of these similar orders.

47. The next step is more difficult and involves establishing the **scope** of *certiorari* review available in these circumstances.

48. It is well established that, within the context of criminal trial proceedings, *certiorari* is only available when the lower court commits “jurisdictional error.” A court will fall into jurisdictional

⁶⁴ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97, 99-100.

⁶⁵ See *textPlus Inc. (Re)*, [2022] O.J. No. 4959 at paras. 40-41; *R. v. Comtois*, 2017 QCCA 1376 at para. 16.

⁶⁶ See e.g. *textPlus Inc. (Re)*, [2022] O.J. No. 4959 at paras. 38-39 (Sup. Ct.); *R. v. Brown*, 2019 ONSC 5032 at para. 17. See also *Alberta (Attorney General) v. Provincial Court of Alberta*, 2015 ABQB 728; *British Columbia (Attorney General) v. Brecknell*, 2018 BCCA 5.

error if it errs in its interpretation of a statute that is jurisdictional in nature; refuses to exercise its jurisdiction; or acts in breach of the principles of natural justice.⁶⁷

49. However, the applicant respectfully contends that, while the law remains unsettled, the scope of *certiorari* review in the context of a *refusal to grant* an application for an order relating to a *Criminal Code* investigative tool ought to be broader.⁶⁸ Several recent cases suggest that, in this context, *certiorari* review is available to the Crown based on either a jurisdictional error *or* an error of law. For example:

- *textPlus Inc. (Re)*: the Superior Court of Justice in Brampton considered both a jurisdictional error and an error of law in finding that *certiorari* relief was available from a provincial court’s refusal to grant a production order. The court suggested but did not decide that an error of law alone is a sufficient basis for *certiorari* relief.⁶⁹
- *Brown*: the Superior Court of Justice in Ottawa granted *certiorari* relief from a provincial court judge’s refusal to grant a search warrant based on an error of law “which prevented the determination of the charges on their merits.”⁷⁰
- *Provincial Court of Alberta*: the Court held that *certiorari* relief from a refusal to issue a production order could be granted if the application judge incorrectly interpreted and applied the relevant provisions of the *Criminal Code*.⁷¹
- *Brecknell*: the Supreme Court of British Columbia dismissed a Crown application for *certiorari* after considering whether the provincial court had committed either a

⁶⁷ See *R. v. Awashish*, [2018 SCC 45](#) at paras. 11, 20, 23; *R. v. Russell*, [\[2001\] 2 S.C.R. 804](#) at para. 19; *Skogman v. The Queen*, [\[1984\] 2 S.C.R. 93](#) at para. 5; *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at para. 40 (Sup. Ct.); *R. v. Jackson*, [2015 ONCA 832](#) at paras. 32-39.

⁶⁸ *R. v. Comtois*, [2017 QCCA 1376](#) at para. 16 (“There has been some uncertainty in the jurisprudence whether error on the face of the record is a valid ground for the issuance of *certiorari* in relation to decisions relating to the authorization of search warrants by justices of the peace. There has been further uncertainty, if it is a valid remedy, as to what constitutes error of law on the face of the record in criminal proceedings. . . .”).

⁶⁹ *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at paras. 40-48 (Sup. Ct.) (stating that “[f]or a *certiorari* application in relation to a refusal by a provincial court to grant an application for an order relating to a *Criminal Code* investigation tool, the law is not clearly settled”).

⁷⁰ *R. v. Brown*, [2019 ONSC 5032](#) at paras. 7, 17.

⁷¹ *Alberta (Attorney General) v. Provincial Court of Alberta*, [2015 ABQB 728](#) at para. 43.

jurisdictional error or error of law in refusing to grant a production order. The B.C. Court of Appeal allowed the Crown appeal based on an error of law alone.⁷²

- *Reference re Criminal Code s. 487.02*: The question presented was whether a transmission data recorder warrant can be assisted by an assistance order under s. 487.02. The provincial court judge who reviewed the application declined to issue the requested order on the basis that it was not permitted under the *Code*. The Crown sought *certiorari* and *mandamus* and argued (as the applicant does here) that the judge misinterpreted the relevant statutory provisions. The Court of Appeal for Newfoundland and Labrador agreed and granted the requested relief.⁷³

50. The Crown is aware of one case that has rejected this approach. In *Provincial Court of Saskatchewan*, the court dismissed a Crown application for *certiorari* from a refusal to grant a search warrant despite finding that the refusal was grounded in legal error. The court held that *certiorari* is only available to parties in criminal proceedings for jurisdictional error.⁷⁴

(2) Analysis

51. Although it is the applicant's position that the alleged errors in the application judge's ruling constitute both jurisdictional error and errors of law, the applicant nevertheless respectfully requests that, consistent with the more expansive historical nature of prerogative *writs*,⁷⁵ the Court confirm that *certiorari* review is available to the Attorneys General in the context of a refused warrant application for an error of law alone.

52. *Certiorari* review for an error of law is appropriate in the context of a refused *ex parte* warrant application for the following reasons.

53. **First**, the usual justification for preventing broad access to *certiorari* does not exist in this context, as there is no risk that *certiorari* review for an error of law will be "used to do an 'end-run' around the rule against interlocutory appeals".⁷⁶ Here, as noted above, it is already open to an

⁷² *British Columbia (Attorney General) v. Brecknell*, [2018 BCCA 5](#) at paras. 18, 60 (citing *British Columbia (Attorney General) v. Brecknell*, 2017 BCSC 460 at para. 45)

⁷³ *Reference re Criminal Code s. 487.02*, [2019 NLCA 6](#) at paras. 1-7.

⁷⁴ *R. v. Provincial Court of Saskatchewan*, [2022 SKQB 184](#) at paras. 2, 27-36.

⁷⁵ See *R. v. Russell*, [\[2001\] 2 S.C.R. 804](#) at para. 19.

⁷⁶ *R. v. Awashish*, [2018 SCC 45](#) at para. 11.

affiant to seek a *de novo* hearing of a rejected general warrant application before a different provincial or superior court judge based on the same ITO. *Certiorari* with *mandamus* relief based on an error of law is – if anything – a more *onerous* and *limited* avenue of obtaining a general warrant than the one that is already available (*i.e.*, an entirely *de novo* application). And unlike *certiorari* applications made while trial is underway, there is no risk that *certiorari* review from a general warrant refusal will *fragment* an ongoing trial or cause undue disruption. Nor does it risk having issues decided without the benefit of a full evidentiary record.⁷⁷

54. **Second**, general warrant applications almost invariably proceed on an *ex parte* basis and rulings on these applications are typically made without submissions on any legal questions that might arise. Despite this, an application judge may release written reasons on a question of law raised by the application, as was done here. That ruling will then bind courts of coordinate jurisdiction.⁷⁸ Since there is no right of appeal from the refusal of a general warrant, there is no avenue to correct alleged legal errors (apart from the Attorney General seeking leave under s. 40 of the *Supreme Court Act* – a narrow, exceptional, and discretionary form of review). *Certiorari* review for an error of law permits the Attorney General to do just that. To ensure a balanced process, a reviewing court can always order notice or appoint *amicus* if desirable and appropriate.

55. **Third**, the discretionary nature of *certiorari* alleviates any concern that permitting review for simple errors of law in the general warrant context would generate results inconsistent with the limited nature of the extraordinary writ. A reviewing court can always deny the remedy – even in the face of clear legal error – if the interests of justice so require.⁷⁹

56. **Fourth**, and finally, an expanded scope of *certiorari* review is consistent with the approach that applies in an analogous context – when a *third party* to a trial proceeding is affected by a mid-trial ruling or search warrant or similar investigative tool.⁸⁰ In such circumstances, the ruling is considered final *vis-à-vis* the third party. It has no ability to apply to the trial judge for relief, and no right to appeal the order at the end of trial. The law thus permits the third party to seek review of the order in superior court through an application for *certiorari* – on an expanded scope of

⁷⁷ *R. v. Awashish*, [2018 SCC 45](#) at paras. 10-12, 17.

⁷⁸ *R. v. Sullivan*, [2022 SCC 19](#) at para. 6; *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at paras. 33-37 (Sup. Ct.).

⁷⁹ *R. v. M.N.*, [2022 ONCA 358](#) at para. 41.

⁸⁰ See e.g. *R. v. Vice Media Canada Inc.*, [2017 ONCA 231](#) at para. 20, *aff'd* [2018 SCC 53](#).

review – that accounts for mere errors of law apparent on the face of the record.⁸¹ The denial of a general warrant (or any other *Criminal Code* search authority) presents the exact same problem for the Attorney General. Although re-application by the police is possible, the denial is a final adverse order for the prosecution that can result in the termination of proceedings. An enlarged standard of review is appropriate.

B. The application judge committed jurisdictional and legal error

57. Even if the Court finds that the more limited “jurisdictional error” standard applies, the Attorney General for Ontario submits that it can still obtain *certiorari* and *mandamus* here.

58. The Attorney General for Ontario respectfully contends that the application judge made the following jurisdictional error: The judge misconstrued the jurisdictional reach of the general warrant provision when he refused to issue the warrant because he felt its objective was outside the permissible bounds of the provision.⁸² Here, the judge described the technique as akin to the one used by “the famed heroic villain Robin Hood.” In his view, the police were using a search tool for “future victim compensation.”⁸³ And while a “laudable” objective, the application judge found it “stretched” the general warrant power beyond its reach.⁸⁴

59. The judge came to this conclusion because, in his view, there are other provisions contained in the *Criminal Code* specifically designed to allow the police to restrain proceeds of crime. As a result, these alternative options limit the reach of a general warrant and its ability to seize proceeds because one of the statutory preconditions or “preliminary questions” for a general warrant is that there be “no other provision” to authorize the technique at issue (s. 487.01(1)(c)).⁸⁵

⁸¹ *R. v. Awashish*, [2018 SCC 45](#) at para. 12; *L.L.A. v. A.B.*, [\[1995\] 4 S.C.R. 536](#) at paras. 23-24, L’Heureux-Dubé J. (“In the case of third parties, they can appeal court orders affecting them before the end of the trial through two procedural avenues. . . . A provincial court order is to be challenged through an enlarged remedy of *certiorari*, which falls within the ambit of superior courts.”); *Dagenais v. Canadian Broadcasting Corp.*, [\[1994\] 3 S.C.R. 835](#) at paras. 17, 38-43, 56; *R. v. Primeau*, [\[1995\] 2 S.C.R. 60](#) at paras. 10-16; *R. v. Jobin*, [\[1995\] 2 S.C.R. 78](#) at para. 28.

⁸² See *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at para. 25 (Sup. Ct.) (holding that a provincial court commits jurisdictional error when it misconstrues the jurisdictional reach of an investigative tool). See also *R. v. Vasarhelyi*, [2011 ONCA 397](#) at para. 52 (stating that jurisdictional error can arise out of a lower court’s failure to “perform a duty”); *R. v. Palacios* (1984), [10 C.C.C. \(3d\) 431](#) at para. 35 (Ont. C.A.) (holding that a lower court commits jurisdictional error when it makes an error of law on a preliminary question that prevents a determination of a case on the merits).

⁸³ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99.

⁸⁴ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97-99.

⁸⁵ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97-99. See also *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at para. 25 (Sup. Ct.); *R. v. Palacios* (1984), [10 C.C.C. \(3d\) 431](#) at para. 35 (Ont. C.A.).

60. The Attorney General for Ontario respectfully suggests that there are three problems with this reasoning, and that the application judge committed jurisdictional error in limiting the scope of the general warrant provision and refusing to issue the proposed technique (that ought to have issued) because he felt it was aimed toward an impermissible purpose.⁸⁶ **First**, investigative search warrants **are** used to seize proceeds of crime; that purpose is not beyond their reach. **Second**, the judge’s reasoning misinterprets the “no other provision” requirement, and that misinterpretation led to an inappropriate jurisdictional limit on the reach of general warrants. And **third**, when the “no other provision” test is properly applied, there are in fact no other alternatives for police to carry out the proposed technique. Each alleged error is taken in turn.

(1) The seizure of proceeds

61. The application judge expressed a view throughout the reasons that the use of a general warrant for “the sole purpose of future compensation” would “stretch” their investigative scope too far.⁸⁷ In his view, the seizure of proceeds was beyond their jurisdictional reach.

62. On this point, the Attorney General for Ontario respectfully disagrees. The caselaw is replete with examples in which traditional investigative warrants have been used by police to recover proceeds of crime, to be subsequently disposed of in accordance with the procedure set out in the *Code*.⁸⁸ This is all the police were doing here. But, in fact, the *Code* goes even further and assumes that there are times when the police may use an investigative warrant to seize property and, without ever seeking a detention order and engaging the disposition process, “return the thing seized . . . to the person lawfully entitled to its possession” when “there is no dispute as to who is lawfully entitled to possession”⁸⁹ Just as the police can use a warrant to enter a *physical* place and recover stolen *physical* goods (like a diamond ring or a vehicle or cash), so, too, can they use

⁸⁶ *R. v. Morelli*, [2010] 1 S.C.R. 253 at para. 40; *R. v. Araujo*, [2000] 2 S.C.R. 992 at paras. 52-56; *Re Church of Scientology (No. 6)* (1987), 31 C.C.C. (3d) 449 at pp. 490-94.

⁸⁷ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99.

⁸⁸ See e.g. *R. v. Floward Enterprises Ltd.*, 2017 ONCA 448 at para. 1 (“As part of a criminal investigation, Toronto police seized a valuable diamond from a pawnbroker, believing it was stolen property. They retained the diamond for the duration of the criminal proceedings.”); *R. v. Hobeika*, 2020 ONCA 750 at paras. 22-25; *R. v. Ha*, 2009 ONCA 340 at para. 11 (upholding a general warrant designed to allow police to conduct a covert entry, search the premises, obtain evidence, and “identify assets which constitute proceeds of crime”); *R. v. Wilson* (1993), 86 C.C.C. (3d) 464 (Ont. C.A.); *Ontario (Attorney General) v. 269 Weldrick Road West*, 2020 ONSC 4605 at para. 6; *R. v. Alves*, [2015] O.J. No. 770 at paras. 1-7 (Sup. Ct.); *R. v. Chanmany*, 2013 ONSC 1937 at para. 1.

⁸⁹ *Criminal Code*, R.S.C. 1985, c. C-46, s. 489.1(1).

an investigative warrant to recover stolen *digital* assets. There is no difference but for their electronic form.

(2) The “no other provision” requirement

63. Section 487.01(1)(c) provides that a general warrant may only issue if “there is no other provision . . . that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.”⁹⁰

64. The provision does *not* impose a requirement of “investigative necessity” – meaning the only way that the police can accomplish their *objective* is *via* a general warrant. ***That is not the test.*** The fact that there are alternative techniques available that might accomplish the same investigative purpose or goal does not preclude the issuance of a general warrant. The police are not required to exhaust all alternative methods of achieving their purpose before resorting to a general warrant.⁹¹

65. Instead, the issue is whether the specific investigative *procedure* sought in the general warrant is authorized by another provision. Properly construed, the test is one of “substantive equivalence.” The issuing judge “must consider the investigative technique that the police seek to utilize with an eye to its actual substance and not merely its formal trappings”.⁹²

66. A hypothetical helps illustrate how this requirement works in practice. Consider a situation in which the police believe that a drug dealer is running a “grow-op” out of their home. The police may seek to confirm this belief with (1) a production order for electrical records⁹³; (2) a s. 487 search warrant to enter the residence⁹⁴; and/or (3) a general warrant to go onto the premises and conduct a “sneak and peak”.⁹⁵ The fact that the police can accomplish their objective in a variety of ways does not preclude reliance upon a general warrant.

⁹⁰ *Criminal Code*, R.S.C. 1985, c. C-46, s. 487.01(1)(c).

⁹¹ *R. v. TELUS Communications Co.*, 2013 SCC 16 at para. 102 (Moldaver J.A., concur.); *R. v. Brown*, 2021 ONCA 540 at paras. 51-54; *R. v. Ha*, 2009 ONCA 340 at paras. 42-44, 52.

⁹² *R. v. TELUS Communications Co.*, 2013 SCC 16 at para. 20 (Abella J.A., maj.); *ibid.* at paras. 71-72, 77, 102 (Moldaver J.A., concur.); *R. v. Brown*, 2021 ONCA 540 at para. 53; *R. v. Strong*, 2020 ONSC 7528 at paras. 111-12.

⁹³ *R. v. Orlandis-Habsburgo*, 2017 ONCA 649.

⁹⁴ *R. v. Vu*, [2013] 3 S.C.R. 657.

⁹⁵ *R. v. Ha*, 2009 ONCA 340 at paras. 39-44.

67. The Attorney General for Ontario respectfully submits that the application judge erred in applying this settled approach to the “no other provision” requirement, as he treated the criterion as one of investigative necessity and then used it to place a jurisdictional limit on the provision.

68. As noted above, the application judge repeatedly characterized the goal of this particular general warrant as the recovery of property for the “sole purpose” of victim compensation.⁹⁶ He then went on to consider whether this *purpose* could be achieved pursuant to another legal mechanism. To that end, the application judge found that a s. 462.33 restraint order was a “reasonable legal alternative” to a general warrant because it prohibited the cryptocurrency exchange from “disposing of, or otherwise dealing with, any interest in the property specified in the order”.⁹⁷ The judge then concluded that the general warrant provision cannot extend to “recovering property obtained by the commission of an offence” – as, in the judge’s view, “there are . . . already a variety of legal mechanisms which would have authorized that,” *i.e.*, the restraint order provisions.⁹⁸

69. The approach misapprehends the inquiry as one of “investigative necessity” (asking whether a restraint order can accomplish the same outcome) rather than focusing on the “investigative procedure” (asking whether a restraint order permits the same investigative technique). Instead of considering whether a restraint order is substantively equivalent to an order transferring the subject cryptocurrency into a police-controlled wallet *as a legal matter*, he considered whether a restraint order could achieve the *goal* of recovering the stolen funds. The judge failed to direct his mind altogether to the *legal* question of whether there was “no other provision” authorizing the technique, as required by s. 487.01. This is contrary to the governing jurisprudence,⁹⁹ and goes beyond the level of mere legal error.¹⁰⁰ Where a judge proceeds on an entirely erroneous basis in law, and in turn frustrates the mandate issued by Parliament by limiting the reach of an investigative tool, the error is jurisdictional.¹⁰¹

⁹⁶ See e.g. Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99.

⁹⁷ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-99.

⁹⁸ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 98.

⁹⁹ *R. v. TELUS Communications Co.*, [2013 SCC 16](#) at para. 102 (Moldaver J.A., concur.); *R. v. Strong*, [2020 ONSC 7528](#) at para. 109.

¹⁰⁰ Compare *P.C. v. Ontario (Attorney General)*, [2020 ONCA 652](#) at para. 35; *R. v. Vasarhelyi*, [2011 ONCA 397](#) at para. 52.

¹⁰¹ *Dubois v. The Queen*, [\[1986\] 1 S.C.R. 366](#) at paras. 21-23; see also *R. v. Sazant*, [\[2004\] 3 S.C.R. 635](#) at para. 25; *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at para. 25 (Sup. Ct.).

(3) The inadequate alternatives

70. The final alleged error is related to the second. The Attorney General for Ontario respectfully submits that, under the correct legal framework, the application judge erred in finding that the police have access to a legal substantive equivalent of a general warrant in this context.

71. The investigative technique at issue is as follows: the police sought a general warrant to transfer cryptocurrency that was stolen as proceeds of crime from Bitcoin addresses associated with the Binance cryptocurrency exchange to a secure wallet held by the DRPS, in order to further the investigation into the alleged offences.¹⁰²

72. Whether this technique would provide the police with “information concerning the offence” is discussed below.

73. Here, it is important to note that the proposed technique was *not* a mere attempt to compensate the victim at the suspects’ expense, as the application judge concluded. Rather, as the ITO made clear, the police merely sought to seize the subject cryptocurrency and bring it under police control and within the disposition regime set out at ss. 489.1 and 490 of the *Code*.¹⁰³ These provisions create an “elaborate scheme” for a criminal court to determine who is lawfully entitled to the seized property – whether it be the victim, the accused, or the state – and to dispose of it as a court considers appropriate. The scheme confers important protections on the person whose items the state holds in detention (*i.e.*, the individuals from whom the cryptocurrency was seized) by, *inter alia.*, providing notice of the seizure and conferring a right on that person to apply for the return of the seized items.¹⁰⁴

74. There is no other statutory authority authorizing this technique. Each of the potential alternative authorizations is addressed in turn. None of the options authorize the same *legal* technique as the general warrant power.

¹⁰² Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 46-53, 90-92.

¹⁰³ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 16, 51 (“My intention is not to restrain the cryptocurrency for the purpose of management and ultimate forfeiture to His Majesty, but rather to investigate the alleged fraud and, if appropriate, return the cryptocurrency to its lawful owner pursuant to s. 489.1(1) and s. 490 of the *Criminal Code*.”)

¹⁰⁴ *Criminal Code*, R.S.C. 1985, c. C-46, [ss. 489.1 and 490](#); *R. v. Garcia-Machado*, [2015 ONCA 569](#) at para. 12-24, 46-56.

(a) Traditional and Special Search Warrants

75. The first potential option is the traditional search warrant powers set out in s. 487 (Search Warrants) and s. 462.32 (Special Search Warrants) of the *Code*. The application judge appeared to agree with the affiant that these provisions do not authorize the technique at issue.¹⁰⁵ As explained above, cryptocurrency exists purely as digital entries on an online ledger or database, known as the blockchain.¹⁰⁶ The traditional search warrant powers apply only to tangible items, not intangible objects like cryptocurrency.¹⁰⁷ Beyond this problem, traditional search warrants are also limited to searching a “building, receptacle or place”.¹⁰⁸ Given the purely digital nature of cryptocurrency and its various public addresses, it is not clear that it exists in a physical location.

(b) Restraint and Management Orders

76. The second possible alternative arises out of the proceeds of crime provisions contained within the *Criminal Code*. It is here that the judge found a viable alternative, stating that “a *Criminal Code* restraining order was **a reasonable legal alternative** to the general warrant sought in this case.”¹⁰⁹ The Attorney General for Ontario respectfully disagrees.

77. There is no doubt that the subject cryptocurrency constitutes “proceeds of crime”, as it is property obtained through the commission of a designated offence.¹¹⁰ Also, the *Criminal Code* does contain provisions dealing specifically with the restraint of proceeds. As the application judge noted, those provisions can, *in certain circumstances*, provide a route for bringing proceeds under state control and returning them to their lawful owner.¹¹¹

78. The procedure operates as follows: In order to secure and dispose of proceeds in cases in which there is no underlying criminal conviction, the Attorney General needs to obtain three separate orders *via* Crown applications, namely: (1) a **restraint order** to secure the funds (s. 462.33); (2) a **management order** permitting a named person to take control over the restrained

¹⁰⁵ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 49-51.

¹⁰⁶ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 18-19.

¹⁰⁷ *Québec (Procureur général) c. Banque Royale du Canada*, [1985] J.Q. no 659 at paras. 6-8; *R. v. Wong* (1987), 34 C.C.C. (3d) 51 at p. 61 (Ont. C.A.).

¹⁰⁸ See *Criminal Code*, R.S.C. 1985, c. C-40, ss. 462.32, 487.

¹⁰⁹ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 98.

¹¹⁰ *Criminal Code*, R.S.C. 1985, c. C-46, s. 462.3(1) (definitions).

¹¹¹ *Criminal Code*, R.S.C. 1985, c. C-46, Part XII.2. See also Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-100.

property (s. 462.331); and then (3) *a forfeiture or return order* to dispose of the property to the state or its lawful owner (ss. 462.331(7.1) or 462.43(1)(c)).

79. On its face, the process seems burdensome but attainable. It is not. And more importantly, it is not the substantive *legal* equivalent of a general warrant in this context.

80. **First**, the general warrant provision permits “*a peace officer* . . . to use [a proposed] *investigative* technique . . . if . . . there is no other provision . . . permitting the technique.”¹¹² Restraint and management orders are not *police* applications, and they are not *investigative* in nature. They may only be made on an application of the Attorney General,¹¹³ and with an Attorney General undertaking “with respect to the payment of damages or costs.”¹¹⁴ Their purpose is to preserve property.¹¹⁵ The two applications are entirely different in nature, and a procedure available only to the Attorneys General for a non-investigative purpose cannot satisfy the “no other provision” requirement of the statutory text. The point is made even more stark when considered from the police perspective. For the affiant’s purposes, it does not help advance the investigation to say that she cannot pursue a technique because an entirely separate, independent state entity *could* decide to do something similar – so long as it has a different purpose in mind.¹¹⁶

81. **Second**, a restraint order does not permit the same investigative technique. Here, the affiant wants to bring the proceeds into police control by virtue of a single judicial application. A restraint order does not do that. It freezes the funds but leaves them under the control of the exchange.¹¹⁷ To be sure, an Attorney General could take further steps – and file an entirely separate, additional application for a management order – asking a court to appoint someone else to take control over and “manage” the cryptocurrency.¹¹⁸ But this multi-step Attorney General-led process is not the same one that would result from the single-step police-driven warrant approach. It also is not what the police want to do. The affiant does not want to “manage” the cryptocurrency – *e.g.*, sell,

¹¹² *Criminal Code*, R.S.C. 1985, c. C-46, s. [487.01\(1\)](#) (emphases added).

¹¹³ *Criminal Code*, R.S.C. 1985, c. C-46, ss. [462.33](#), [462.331\(1\)](#).

¹¹⁴ *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.33\(7\)](#).

¹¹⁵ *R. v. Am-Stat Corp.*, [2011 ONSC 7462](#) at para. 40 (“The purpose of the Restraint and Management provisions is to preserve property until a forfeiture application can be brought and decided.”).

¹¹⁶ See *R. v. McNeil*, [\[2009\] 1 S.C.R. 66](#) at para. 23 (“Under our Canadian system of law enforcement, the general duty to investigate crime falls on the police, not the Crown. The fruits of the investigation against an accused person, therefore, will generally have been gathered, and any resulting criminal charge laid, by the police. [T]he roles of the Crown and the police are separate and distinct . . .”).

¹¹⁷ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 50-51.

¹¹⁸ See *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.331\(1\)](#).

destroy, return, or forfeit the funds¹¹⁹ – but rather simply wants to hold it pending a judicial determination as to its lawful owner.¹²⁰

82. **Third**, as set out by the affiant, a restraint order is **not even available** in this context. In order for the Attorney General to obtain a restraint order *vis-à-vis* proceeds, the application must demonstrate that there are reasonable grounds to believe that “an order of forfeiture may be made under subsections 462.37(1) or (2.01) or 462.38(2) in respect of the property.”¹²¹

83. That requirement presents an insurmountable hurdle. A forfeiture order under these provisions can **only** issue upon the laying of charges or after a finding of guilt in a successful domestic prosecution.¹²² As discussed, cryptocurrency-related offences are not confined by traditional territorial borders and are often committed entirely in cyberspace. As the application judge accepted, investigations into these offences “typically involve transnational entities and foreign suspects”¹²³ and, as such, cybercrime suspects are frequently outside the reach of Canadian authorities. Extradition is rare. The likelihood of Canadian charges being laid is remote. Certainly, there is no reason to think that charges here are likely. To the contrary, the application judge put this point in the starkest of terms: “There is **nothing** in the application which suggests that the investigation has come close to being able to arrest and prosecute the foreign suspects.”¹²⁴

84. In such circumstances, a restraint order is simply unavailable as a matter of law. There is no prospect of an indictment. No hope of a conviction. No chance for forfeiture. No opportunity for restraint.¹²⁵ A restraint order is not an adequate alternative to the investigative technique at issue because the grounds for obtaining such an order do not exist.

85. **Fourth**, restraint orders for proceeds are *time limited*. They expire after six months unless charges are laid.¹²⁶ Thus, assuming they are available and a viable tool for restraining

¹¹⁹ *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.331\(1\)-\(3\)](#).

¹²⁰ See e.g. Affidavit of Taryn Snow, Exhibit A: ITO, at p. 16.

¹²¹ *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.33](#).

¹²² For proceeds of crime, forfeiture orders are made under [s. 462.37\(1\)](#) or [s. 462.37\(2.01\)](#) (requiring a finding of guilt for a designated offence); or [s. 462.38\(2\)](#) (requiring an information to have been laid and the accused be deemed to have absconded). Likewise, for a restitution order under [s. 738](#), the accused must be “tried for an offence”, and the court must determine that an “offence has been committed” prior to any order returning the property to victims.

¹²³ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97.

¹²⁴ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 97 (emphasis added).

¹²⁵ *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.33](#).

¹²⁶ *Criminal Code*, R.S.C. 1985, c. C-46, s. [462.35\(1\)](#).

cryptocurrency held by an exchange, such orders only present an “*interim* remedy” – as the application judge had to acknowledge.¹²⁷ (There is an argument that this six-month limitation period ends with the acquisition of a management order – though the issue has never been litigated or decided, so far as the Attorney General for Ontario is aware.¹²⁸)

86. **Fifth**, for any restraint order to have effect and impose a (temporary) freeze on the disposition of the proceeds, the state will require the *ongoing* cooperation and compliance of the exchange storing the digital assets. If an exchange lifts its freeze in breach of a restraint order, the police would have little recourse to secure the cryptocurrency against dissipation. And while, as the application judge noted, the cryptocurrency exchange involved in this investigation (Binance) is currently compliant with Canadian court orders, this may not always be the case.¹²⁹

87. The application judge labelled this suggestion as “entirely illogical.”¹³⁰ He found the risk of an exchange complying with a general warrant but unilaterally terminating a restraint non-existent. If they will comply with one order, why not the second?

88. The reason is that an effective restraint order requires *ongoing* or *continued* compliance over time and, when it comes to Binance (and other cryptocurrency exchanges), the risk of future non-compliance is *very* real. As a general matter, cryptocurrency exchanges are often involved in serious disputes surrounding their regulatory compliance.¹³¹ In Canada, for Binance, such disputes occur frequently. For example, *just weeks ago*, on May 10, 2023, the Ontario Securities Commission (“OSC”) served Binance with an investigative order authorizing “an extremely broad inquiry into whether Binance may have taken steps to circumvent Ontario securities law and compliance controls”.¹³² Two days later, Binance posted a lengthy statement *via* Twitter stating

¹²⁷ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99 (emphasis added).

¹²⁸ A restraint order under s. 462.33 will expire after a period of six months unless “proceedings are instituted” or the judge is satisfied that the property is required: for the purpose of any provision respecting forfeiture; for the purpose of any investigation; or as evidence in any proceeding: *Criminal Code*, R.S.C. 1985, c. C-46, s. 462.35(1)-(3).

¹²⁹ Affidavit of Taryn Snow, Exhibit A: ITO, at p. 50; Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 98-99.

¹³⁰ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99.

¹³¹ Affidavit of Taryn Snow, Exhibit A: ITO, at p. 50. On March 27, 2023, the U.S. Commodity Futures Trading Commission launched a civil enforcement action against Binance alleging that the company made deliberate, strategic decisions to evade federal law: “[Release Number 8680-23](#)”, *Commodity Futures Trading Commission* (27 March 2023). See also: New York Times, “[S.E.C. Accuses Binance of Mishandling Funds and Lying to Regulators](#)”, (5 June 2023). Similarly, on March 22, 2023, the U.S. Security Exchange Commission issued a notice to the cryptocurrency exchange Coinbase, indicating that regulators believe laws protecting investors were violated: Michelle Chapman, “[Coinbase tumbles after SEC warns of securities violations](#)”, *AP News* (23 March 2023).

¹³² See Bloomberg, “[Binance Discloses Investigation by Canadian Regulator](#)” (31 May 2023).

that it was “joining other prominent crypto businesses in proactively withdrawing from the Canadian marketplace.”¹³³ Likewise, the company had previously pulled out of Ontario in June 2021, in response to an alleged regulatory crackdown by the OSC.¹³⁴ During this same time period other large, prominent, seemingly legitimate cryptocurrency exchanges (*i.e.*, FTX and Quadriga) have simply collapsed into bankruptcy – with few recoverable assets.¹³⁵

89. This risk of non-compliance is exacerbated when the exchange takes the position that they are not subject to Canadian jurisdiction. To that end, Binance has stipulated “that its cooperation and acceptance of [a Canadian court] should not be construed as an admission that it is subject to the jurisdiction of Canadian courts.”¹³⁶ It expressly reserves the right not to comply with Canadian court orders.

(c) The Proposed Digital Assets Amendments

90. As noted above, the government has introduced proposed *Criminal Code* amendments specifically addressing the seizure, management, and disposition of digital assets in the time since the applicant judge’s ruling.¹³⁷ These proposed amendments, while a step in the right direction, still do not authorize the technique covered by the general warrant here. Similar to the existing restraint and management provisions discussed above, in its current form, the proposed special warrant provision for digital assets only applies to digital assets that “may be the subject of an order of forfeiture made under subsection 462.37(1) or (2.01) or 462.38(2)”.¹³⁸ They also require Crown applications. And a multi-step Attorney General-led management process. These proposed amendments for seizing and disposing of cryptocurrency are therefore limited by the same legal and practical challenges affecting the current restraint and management provisions.

¹³³ See Twitter, @Binance, [May 12, 2023, at 3:05 p.m.](#)

¹³⁴ Affidavit of Taryn Snow, Exhibit A: ITO, at p. 25. See also Financial Post, “[Binance’s Exit and Bank of Canada’s digital loonie discussions](#)” (May 16, 2023); Financial post, “[Crypto Platform Binance Quits Canada After Provinces Join Together to Tighten Rules](#)” (May 12, 2023).

¹³⁵ See Wikipedia, [Bankruptcy of FTX](#) (May 31, 2023); Wikipedia, [Quadriga Fintech Solutions](#) (May 31, 2023); Tara Deschamps, “[Crypto exchange Quadriga was a fraud and founder was running Ponzi scheme, OSC report finds](#)”, *The Canadian Press* (11 June 2020); Nathan Reiff, “[The Collapse of FTX: What Went Wrong with the Crypto Exchange?](#)”, *Investopedia* (27 February 2023).

¹³⁶ Affidavit of Taryn Snow, Exhibit A: ITO, at p. 26.

¹³⁷ See Bill C-57, [Budget Implementation Act](#), 2023, No. 1, 1st Sess, 44th Parl, 2023, s. 212.

¹³⁸ See Bill C-57, [Budget Implementation Act](#), 2023, No. 1, 1st Sess, 44th Parl, 2023, s. 212.

91. In any event, these provisions have not yet come into force and there is no guarantee that they will do so. And they could not have precluded reliance on the general warrant provision in this case, as they were not yet in existence.

C. This Court should exercise its discretion to grant *certiorari* with *mandamus*

92. As set out at length above, it is the Attorney General for Ontario's respectful view that the application judge committed jurisdictional error by incorrectly interpreting the "no other provision" requirement and, in so doing, the judge narrowed the jurisdictional reach of the provision in a way that led him to conclude the proposed technique falls outside of its ambit.

93. The Attorney General for Ontario nevertheless acknowledges that *certiorari* review is discretionary and does not issue as of right upon a finding of error.¹³⁹ Still, it submits that there are compelling reasons why this Court should exercise its discretion and grant an order of *mandamus* compelling the lower court to issue the requested orders.

(1) The remaining general warrant criteria are satisfied

(a) The general warrant will provide information concerning the offences

94. Section 487.01(1)(a) requires the issuing judge to be satisfied on reasonable grounds to believe that "information concerning the offence will be obtained" through the technique or procedure sought in the general warrant.

95. The application judge addressed this requirement in passing and, in so doing, fell into the same jurisdictional error noted above. In his words: "it would stretch the intended meaning of . . . 'information' . . . to extend the scope of general warrants to include the seizure of property for the sole purpose of future compensation."¹⁴⁰ As set out above, the Attorney General for Ontario respectfully states there are several flaws in this conclusion: (1) that was not the purpose of the application; (2) the recovery of stolen proceeds does fall within the jurisdictional ambit of the *Criminal Code*'s investigative warrants; and (3) the application judge's analysis improperly focuses the jurisdictional reach of the provision on the *objective* or *purpose* of the warrant rather than on whether it captures the proposed legal technique.

¹³⁹ *R. v. Vasarhelyi*, 2011 ONCA 397 at para. 50.

¹⁴⁰ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99.

96. When correctly applied, “information concerning the offence” is sufficiently broad to capture the technique at issue here.

97. As a legal matter, the phrase takes on an expansive scope, given the flexible range of investigative techniques contemplated by the general warrant provision.¹⁴¹ The Supreme Court has interpreted the corresponding criterion under the s. 487(1) search warrant power, requiring “evidence with respect to the commission of an offence”, as “encompassing **anything relevant or rationally connected** to the incident under investigation, the parties involved, and their potential culpability”.¹⁴² The s. 487.01(1)(a) requirement is then even broader, as it includes “information that is not known to exist at the time the warrant is granted.”¹⁴³

98. Here, the proposed general warrant will yield “information concerning the offence.” Specifically, the police will gain control over the stolen cryptocurrency, which itself is a data entity on an online database (*i.e.*, *information*¹⁴⁴) that is “rationally connected” to the offence as proceeds.¹⁴⁵

99. The general warrant also will provide the police with evidence concerning the alleged offences. To begin, it is a stimulating tactic. It is reasonable to believe that the seizure of cryptocurrency from an exchange address – which will then in turn result in a corresponding depletion of the suspects’ exchange accounts – is likely to trigger a reaction from the account holders, *e.g.*, they may contact police to complain and assert an ownership interest in the proceeds. This very thing has happened in the past.¹⁴⁶ And it can provide evidence for the police that, prior to the seizure, the account holder (and suspect) believed that they were in possession of the proceeds of the offence – connecting them to the alleged crimes. The technique also has potential to generate a conversation with the suspect and additional leads.

100. The general warrant will also provide evidence of the suspect’s connection to the proceeds in a second way. The proposed technique is an order directing the exchange to transfer

¹⁴¹ *R. v. Hoang*, [2021 ONSC 6054](#) at paras. 44-45.

¹⁴² *CanadianOxy Chemicals Ltd. v. Canada (Attorney General)*, [\[1999\] 1 S.C.R. 743](#) at para. 15 (emphasis added).

¹⁴³ *R. v. Hoang*, [2021 ONSC 6054](#) at paras. 44-45. See also *R. v. Wise*, [2020 ONSC 7716](#) at 102-05.

¹⁴⁴ See *Criminal Code*, R.S.C. 1985, c. C-46, s. 342.1(2) (defining “computer data” as “representations, including signs, signals, or symbols, that are in a form suitable for processing in a computer system”); *R. v. Vu*, [\[2013\] 3 S.C.R. 657](#) at paras. 40-45 (describing computer data as “information”).

¹⁴⁵ See *CanadianOxy Chemicals Ltd. v. Canada (Attorney General)*, [\[1999\] 1 S.C.R. 743](#) at para. 15.

¹⁴⁶ See Supplemental Affidavit of Taryn Snow at para. 12.

cryptocurrency that has been identified as proceeds of crime from an exchange-controlled address to one controlled by the police.¹⁴⁷ When the transfer executes, it represents a confirmation, by the exchange, that the subject proceeds were – *in fact* – previously associated to the exchange and, in turn, its account holders suspected of the alleged offences.¹⁴⁸ The transfer provides the police with confirmation of the exchange and suspects’ involvement in the alleged fraud and direct evidence of their alleged possession of what the police say is property obtained by crime.¹⁴⁹

101. It is of course possible that the police could glean similar information about the connection between the proceeds, the exchange, and the suspects through other means, most notably, the blockchain. For example, the police could trace the flow of the stolen funds into public addresses controlled by the exchange using the public blockchain and then identify the account holders associated with the funds by using a production order. (The police did that here.)

102. This does not preclude a general warrant application, however. The blockchain provides useful information but the transfer of funds *confirms* that information beyond any doubt. As a legal matter, the “no other provision” requirement applies to the proposed *method* of obtaining the information, not the *uniqueness* of the information being sought. A general warrant may issue even if the information sought could be obtained *via* some other route.¹⁵⁰

103. And that makes sense, as there is often a need for the police to corroborate their investigative beliefs through multiple sources of information. (For example, if the police only had this information by reviewing the online blockchain, it is unclear how they could prove what they know in court – given the decentralized nature of the record; the difficulty in authenticating it; unfamiliarity with the reliability of blockchain technology; and the fact that blockchain records do not obviously meet the test for admissibility as a business record.¹⁵¹) Regardless, at the stage of considering an application for a warrant, it is not the issuing judge’s role to assess whether the

¹⁴⁷ See Supplemental Affidavit of Taryn Snow at paras. 4, 26.

¹⁴⁸ See Supplemental Affidavit of Taryn Snow at paras. 25-26.

¹⁴⁹ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99 (“[T]he application may have shown that the targeted proceeds probably belong to the suspects who defrauded the victim.”).

¹⁵⁰ *R. v. Strong*, [2020 ONSC 7528](#) at para. 110; *R. v. TELUS Communications Co.*, [2013 SCC 16](#) at para. 102 (Moldaver J.A., concur.); *R. v. Brown*, [2021 ONCA 540](#) at paras. 51-54; *R. v. Ha*, [2009 ONCA 340](#) at paras. 42-44, 52.

¹⁵¹ See *Canada Evidence Act*, R.S.C. 1985, c. C-5, [s. 30](#).

police already “have enough” to prove the charges. There is no “investigative necessity” requirement for a general warrant to issue.¹⁵²

(b) The general warrant is in the best interests of the administration of justice

104. Section 487.01(1)(b) also requires that the proposed warrant be “in the best interests of the administration of justice.” The analysis engages two components: consideration of whether the warrant would further the objectives of justice; and balancing the interests of effective law enforcement against the individual’s interest in privacy.¹⁵³

105. The Attorney General for Ontario respectfully submits that the test is satisfied here. There is no dispute that there are grounds to believe the subject cryptocurrency constitutes proceeds.¹⁵⁴ It is frozen but merely outside of state control. As set out above, its transfer would further the investigation into the alleged offences and allow its ultimate disposition pursuant to the strict procedure set out in the *Code* – which could include its return to the target addresses. Its seizure also would further the vital state interest in addressing the growing threat to Canadians caused by the plague of online cybercrime, as detailed above.¹⁵⁵

106. The application judge appears to have accepted this reality but nevertheless found that the requirement was not satisfied, again, for the same jurisdictional reasons described above, *i.e.*, the use of a general warrant to recover proceeds for future victim compensation is unlawful.¹⁵⁶ For the reasons set out above, the Attorney General for Ontario respectfully contends that the application judge’s analysis suffers from several fatal flaws (as noted).

107. The application judge also grounded his conclusion on an important factual error. The application judge’s concerns arose – in part – from his finding that the affiant had failed to establish that the cryptocurrency in the target addresses was the *same cryptocurrency* stolen from the victim. He specifically noted that the target addresses held more cryptocurrency at the time of the general warrant application than immediately following the alleged offences. This led him to conclude that

¹⁵² See *R. v. Vice Media Canada Inc.*, [2017 ONCA 231](#) at paras. 39-41

¹⁵³ See *R. v. Nguyen*, [2023 ONCA 367](#) at paras. 45-46. See also *R. v. Finlay and Grellette* (1985), [52 O.R. \(2d\) 632](#) at pp. 654-56 (C.A.); *R. v. Lucas*, [2014 ONCA 561](#) at para. 118; *R. v. Ha*, [2009 ONCA 340](#) at para. 46.

¹⁵⁴ See Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 98.

¹⁵⁵ See Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 52-53; Supplemental Affidavit of Taryn Snow at paras. 7-8.

¹⁵⁶ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at p. 99 (“Use of the general warrant provision by the police to seize suspected fraudulently obtained cryptocurrency from an exchange company for future victim compensation would also risk bringing the administration of justice into disrepute.”).

the police were simply planning to take the suspects' money and give it to the victim, hence the "Robin Hood" reference. The judge held that this was a "laudable" but "unlawful" pursuit.¹⁵⁷

108. This finding was grounded in several related misapprehensions of the cryptocurrency tracing relied upon by the affiant.¹⁵⁸ The ITO shows that the police *only* sought to seize the amount of cryptocurrency that (1) is traceable from the victim into the three target addresses; and (2) has remained frozen by the exchange in the target addresses since shortly after the alleged fraud. The application did not seek to seize an additional or unrelated amount.¹⁵⁹ The police were not simply compensating the victim at the suspects' expense; they were recovering the direct and immediate proceeds of the alleged offences.

109. Lastly, the application judge's conclusion misapprehended the purpose of the general warrant provision by concluding that the "appropriate remedy" in this space was for "Parliament to address the issue."¹⁶⁰ As explained above, general warrants are specifically intended to fill gaps in the legislation by authorizing a technique or procedure not addressed by Parliament.¹⁶¹

(2) There is a national interest in confirming the validity of the general warrant technique

110. It is the Attorney General for Ontario's position that an order of *certiorari* with *mandamus* in this case will serve an essential national purpose. It will confirm the continued availability of general warrants as a method of seizing cryptocurrency from suspect accounts on third-party exchanges – a critical investigative tool in the ongoing fight against cybercrime in this country. There is currently no clear legal mechanism in the *Criminal Code* permitting the police to accomplish the technique being proposed here. Although legislative amendments authorizing cryptocurrency seizures are forthcoming, the proposed amendments are limited in scope and do not provide a substantive equivalent to the technique sought in the general warrant. As such,

¹⁵⁷ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97, 99.

¹⁵⁸ Contrary to the application judge's findings: (1) the suspects did not have 18 months to transfer the victim's cryptocurrency out of the target addresses after the alleged offences as the wallet addresses have been frozen since December 2021; (2) 0.178117 BTC was the total amount of the victim's cryptocurrency that was traced to the *three target addresses*, not the total amount of cryptocurrency that the victim transferred during the fraud; and (3) 0.08022315 BTC was the amount of the victim's cryptocurrency *remaining* in the target addresses when tracing was completed in 2021, not the *total* amount of cryptocurrency in the target addresses at that time: Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 97, 99; Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 35-38.

¹⁵⁹ Affidavit of Taryn Snow, Exhibit A: ITO, at pp. 35-38, 91-92.

¹⁶⁰ Affidavit of Taryn Snow, Exhibit B: Reasons for Judgment, at pp. 99-100.

¹⁶¹ *R. v. TELUS Communications Co.*, [2013 SCC 16](#) at para. 91 (Moldaver J.A., concur.).

general warrants will remain an important and necessary gap-filling tool for police to seize cryptocurrency in cases for which a successful domestic prosecution is unlikely.

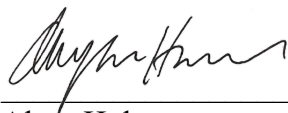
111. The application judge's ruling puts this important technique in jeopardy. It is the *only* published decision about the use of general warrants to seize cryptocurrency, and the decision is arguably binding at the Ontario Court of Justice level.¹⁶² Given the alleged jurisdictional and legal errors in the application judge's reasoning, *certiorari* with *mandamus* relief is required to clarify the continued availability of general warrants to seize cryptocurrency and other digital assets.

PART IV: ORDER REQUESTED

112. The Attorney General for Ontario respectfully requests that the application for an order in the nature of *certiorari* with *mandamus* be granted; that the order of the Honourable Justice Burstein dismissing the applications for a general warrant and related assistance order be quashed; and that an order be made compelling the Provincial Court to exercise its jurisdiction and grant the general warrant and assistance order.

113. In the alternative, the Attorney General for Ontario respectfully requests an order quashing the order of the Honourable Justice Burstein dismissing the applications, and an order remitting the applications to a different justice of the Provincial Court for reconsideration.

All of which is respectfully submitted this 6th day of June, 2023, by



Alysia Holmes
Counsel for the Applicant



Michael Fawcett
Counsel for the Applicant

¹⁶² *R. v. Sullivan*, [2022 SCC 19](#) at para. 6; *textPlus Inc. (Re)*, [\[2022\] O.J. No. 4959](#) at paras. 33-37 (Sup. Ct.).

SCHEDULE A: AUTHORITIES TO BE CITED

Jurisprudence

Alberta (Attorney General) v. Provincial Court of Alberta, [2015 ABQB 728](#)

British Columbia (Attorney General) v. Brecknell, [2018 BCCA 5](#)

CanadianOxy Chemicals Ltd. v. Canada (Attorney General), [\[1999\] 1 SCR 743](#)

Dagenais v. Canadian Broadcasting Corp., [\[1994\] 3 S.C.R. 835](#)

Dubois v. The Queen, [\[1986\] 1 S.C.R. 366](#)

L.L.A. v. A.B., [\[1995\] 4 S.C.R. 536](#)

Ontario (Attorney General) v. 269 Weldrick Road West, [2020 ONSC 4605](#)

P.C. v. Ontario (Attorney General), [2020 ONCA 652](#)

Québec (Procureur général) c. Banque Royale du Canada, [\[1985\] J.Q. no 659](#)

Skogman v. The Queen, [\[1984\] 2 S.C.R. 93](#)

Ward v. University of Prince Edward Island, [1997 CanLII 4643](#) (PE SCTD)

R. v. Alves, [\[2015\] O.J. No. 770](#)

R. v. Am-Stat Corp., [2011 ONSC 7462](#)

R. v. Araujo, [\[2000\] 2 S.C.R. 992](#)

R. v. Awashish, [2018 SCC 45](#)

R. v. Blais, [2008 BCCA 389](#)

R. v. Brown, [2019 ONSC 5032](#)

R. v. Brown, [2021 ONCA 540](#)

R. v. Bond, [2021 ONCA 730](#)

R. v. Campbell, [\[2014\] O.J. No. 6541](#) (Sup. Ct.)

R. v. Chanmany, [2013 ONSC 1937](#)

R. v. Colbourne (2001) [157 C.C.C. \(3d\) 273](#) (Ont. C.A.)

R. v. Comtois, [2017 QCCA 1376](#)

R. v. Domstad, [2001 ABQB 179](#)

R. v. Duchcherer, [2006 BCCA 171](#)

R. v. Finlay and Grellette (1985), [52 O.R. \(2d\) 632](#)

R. v. Floward Enterprises Ltd., [2017 ONCA 448](#)

R. v. Garcia-Machado, [2015 ONCA 569](#)

R. v. Ha, [2009 ONCA 340](#)

R. v. Hoang, [2021 ONSC 6054](#)

R. v. Hobeika, [2020 ONCA 750](#)

R. v. Jackson, [2015 ONCA 832](#)

R. v. Jobin, [\[1995\] 2 S.C.R. 78](#)

R. v. Jodoin, [2018 ONCA 638](#)

R. v. Lucas, [2014 ONCA 561](#)

R. v. M.N., [2022 ONCA 358](#)

R. v. McNeil, [\[2009\] 1 S.C.R. 66](#)

R. v. Morelli, [\[2010\] 1 S.C.R. 253](#)

R. v. Nguyen, [2023 ONCA 367](#)

R. v. Orlandis-Habsburgo, [2017 ONCA 649](#)

R. v. Palacios (1984), [10 C.C.C. \(3d\) 431](#) (Ont. C.A.)

R. v. Persaud, [2016 ONSC 8110](#)

R. v. Primeau, [\[1995\] 2 S.C.R. 60](#)

R. v. Russell, [\[2001\] 2 S.C.R. 804](#)

R. v. Sazant, [\[2004\] 3 S.C.R. 635](#)

R. v. Stewart, [2017 ONSC 7193](#)

R. v. Strong, [2020 ONSC 7528](#)

R. v. Sullivan, [2022 SCC 19](#)

R. v. TELUS Communications Co., [2013 SCC 16](#)

R. v. The Provincial Court of Saskatchewan, [2022 SKQB 184](#)

R. v. Vachon-Desjardins, [2022 ONCJ 43](#)

R. v. Vasarhelyi, [2011 ONCA 397](#)

R. v. Vice Media Canada Inc., [2017 ONCA 231](#) aff'd [2018 SCC 53](#).

R. v. Vu, [\[2013\] 3 S.C.R. 657](#)

R. v. Wilson (1993), [86 C.C.C. \(3d\) 464](#) (Ont. C.A.)

R. v. Wise, [2020 ONSC 7716](#)

R. v. Wong, (1987), [34 C.C.C. \(3d\) 51](#)

Re Church of Scientology (No. 6) (1987), [31 C.C.C. \(3d\) 449](#)

Re Section 487.02 of the Criminal Code, [2019 NLCA 6](#)

textPlus Inc. (Re), [\[2022\] O.J. No. 4959](#)

Secondary Material: Government Documents

Canadian Anti-Fraud Centre, “[Annual Report: 2021](#)”.

Canadian Centre for Cyber Security, “[National Cyber Threat Assessment, 2023-2024](#)”.

Commodity Futures Trading Commission, “[Release Number 8680-23](#)”(27 March 2023).

Bill C-57, [Budget Implementation Act](#), 2023, No. 1, 1st Sess, 44th Parl, 2023, ss. 212-227.

Government of Canada, [Budget 2023](#), Ch. 5.

Government of Canada, [Treaties](#).

Parliament of Canada, [Bill C-57](#).

Secondary Material: Online Sources

Berthiaume, Lee. “[Cyber attack hits engineering giant with contracts for military bases, power plants](#)”, *The Canadian Press* (8 March 2023).

Bloomberg, “[Binance Discloses Investigation by Canadian Regulator](#)” (31 May 2023).

Chapman, Michelle. “[Coinbase tumbles after SEC warns of securities violations](#)”, *AP News* (23 March 2023).

Deschamps, Tara. “[Crypto exchange Quadriga was a fraud and founder was running Ponzi scheme, OSC report finds](#)”, *The Canadian Press* (11 June 2020).

Emisoft Malware Labs (11 February 2020) (Blog); Jade Markus, “[Reported ransomware attacks in Calgary dropped 41% last year](#)”, *CBC News* (11 February 2023).

Fraser, David. “[Digital currency donations for Freedom Convoy evading seizure by authorities](#)”, *CBC Investigates* (21 March 2022).

Financial Post, “[Binance’s Exit and Bank of Canada’s digital loonie discussions](#)” (May 16, 2023).

Financial Post, “[Crypto Platform Binance Quits Canada After Provinces Join Together to Tighten Rules](#)” (May 12, 2023).

Financial Post, “[Safety Net: Crypto scams are duping thousands of Canadians, leaving them despondent and broke](#)” (March 9, 2023).

Financial Post, “[Police have turned crypto seized from trucker convoy over to escrow agent, court told](#)” (9 March 2022).

Markus, Jade. “[Reported ransomware attacks in Calgary dropped 41% last year](#)”, *CBC News* (11 February 2023).

McPhee, Emma. “[Gone Phishing: Cyber crime on rise in Canada, and it’s proving costly](#)”, *Postmedia News* (1 March 2023).

New York Times, “[S.E.C. Accuses Binance of Mishandling Funds and Lying to Regulators](#)”, (5 June 2023).

Northcott, Paul. “[Countering the rise of cryptocurrency fraud](#)”, *RCMP Gazette* (23 March 2022).

Northcott, Paul. , “[Police help victim of crypto-fraud get money back](#)”, *RCMP Gazette* (10 May 2022).

Ontario Securities Commission, “[Crypto 101: Glossary](#)”.

Osler, “[Anti-Money Laundering Rules for Cryptocurrency dealers finalized by Canadian Government](#)” (July 12, 2019).

RCMP, “[RCMP Cybercrime Strategy](#)” (December 2, 2015).

Reiff, Nathan. “[The Collapse of FTX: What Went Wrong with the Crypto Exchange?](#)”, *Investopedia* (27 February 2023).

Tumilty, Ryan. “[This could be the worst year ever for ransomware attacks: experts](#)”, *The National Post* (1 February 2023).

“[The Fifth Estate: Hunting the Hacker of Gatineau](#)”, *CBC News* (7 November 2022).

Twitter, @Binance, [May 12, 2023, at 3:05 p.m.](#)

Wikipedia, [Bankruptcy of FTX](#) (May 31, 2023)

Wikipedia, [Quadriga Fintech Solutions](#) (May 31, 2023)

Wired, “[Cryptocurrency’s Myth of Anonymity](#)” (Feb. 9, 2023).

SCHEDULE B: RELEVANT LEGISLATIVE PROVISIONS

Canada Evidence Act, R.S.C. 1985, c. C-5, [s. 30](#).

SUPERIOR COURT OF JUSTICE
(Central East Region)

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

FACTUM OF THE APPLICANT

Ministry of the Attorney General
Crown Law Office – Criminal
720 Bay Street, 10th Floor
Toronto, Ontario, M7A 2S9

Alysa Holmes
Counsel for the Applicant
Tel: (437) 288-2793
Alysa.Holmes@ontario.ca

Michael Fawcett
Counsel for the Applicant
Tel: (416) 268-4342
Michael.Fawcett@ontario.ca



Law Society
of Ontario

Barreau
de l'Ontario

TAB 1

Anti-Money Laundering: Protecting Your Litigation Practice

Cryptocurrency Considerations

Factum of the *Amicus Curiae*

Michael W. Lacy and Bryan Badali

Brauti Thorning LLP

Submitted by: Michael Fawcett, Crown Law Office – Criminal

Ministry of the Attorney General

October 17, 2023



**ONTARIO
SUPERIOR COURT OF JUSTICE**
(Central East Region)

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

FACTUM OF *AMICUS CURIAE*

BRAUTI THORNING LLP

2900 – 161 Bay St.
Toronto, ON M5J 2S1

Michael W. Lacy

Tel: (416) 360-2776

mlacy@btlegal.ca

Bryan Badali

Tel: (416) 360-2777

bbadali@btlegal.ca

Amicus Curiae

**TO: MINISTRY OF THE ATTORNEY GENERAL
CROWN LAW OFFICE – CRIMINAL**
720 Bay Street, 10th Floor
Toronto, ON M7A 2S9

Michael Fawcett / Alysa Holmes
Tel: 416.326.4600
Fax: 416.326.4656
Email: Michael.Fawcett@ontario.ca
Alysa.Holmes@ontario.ca

Crown Counsel

AND TO: BORDEN LADNER GERVAIS LLP
Bay Adelaide Centre, East Tower
22 Adelaide Street West, Suite 3400
Toronto ON M5H 4E3

Graeme Hamilton
Tel: 416.367.6746
Fax: 416.367.6749
Email: ghamilton@blg.com

Counsel for the Respondent,
Binance Holdings Limited

INDEX

I. STATEMENT OF THE CASE	1
II. FACTUAL CONTEXT.....	3
A. Overview.....	3
B. The Information to Obtain	4
1) The Reasonable Grounds to Believe an Offence was Committed	4
2) The Investigation.....	5
3) The Grounds for a General Warrant	6
C. The Proposed Order	8
D. The Application Judge’s Endorsement.....	8
E. The Supplementary Affidavit of D/C Snow.....	10
III. ISSUES AND THE LAW	12
A. The General Warrant Provision.....	12
B. The Availability of <i>Certiorari Review</i>	13
C. The Applicant’s Claims of Jurisdictional & Legal Error	15
1) The Use of s. 487 and s. 487.01 Warrants to Seize Proceeds of Crime	15
2) There are Other Legislative Regimes Governing the Proposed Procedure – s.487.01(1)(c).....	19
3) The Proposed Procedure Will Not Furnish “Information Concerning the Offence” – s.487.01(1)(a).....	30
4) Authorizing the Proposed Procedure by Means of a General Warrant is not in the Best Interests of Justice – s.487.01(1)(b).....	33
D. CONCLUSION.....	36
IV. LIST OF AUTHORITIES	38

I. STATEMENT OF THE CASE

1. In the last decade, cryptocurrency has become an increasingly popular financial tool. Investment vehicle, stateless alternative to fiat currencies, the promises of cryptocurrency are as limitless as the perils. There can be no doubt that, like many others, criminals have turned to cryptocurrency to facilitate their misdeeds. In the years to come, the anonymous and ethereal nature of cryptocurrency will likely pose challenges to traditional concepts in criminal law, including proof of identity and control. That cryptocurrency may pose novel legal issues in some respects, however, does not necessarily preclude the application of existing tools for search and seizure. Substance must prevail over form.

2. This application raises a legal question of significant import beyond the particular request that was made by the Durham Regional Police Service (“DRPS”): Where police seek to take control of cryptocurrency located in a “wallet” held on a third-party public exchange, does the unique structure of cryptocurrency oust the existing provisions of the *Criminal Code* dealing with restraint and management of proceeds of crime (ss. 462.33 and 462.331) and/or offence-related property (s. 490.8)? And, although the answer to that question is important (although not necessarily controlling) to the resolution of the prerogative writ brought by the Crown, the narrower question is whether Justice Burstein exceeded his jurisdiction in refusing to grant the application for a General Warrant brought under s.487.01 of the *Criminal Code*.

3. The position of *Amicus curiae* with respect to these two questions is as follows:

- 1) Sections 462.33 and 462.331 of the *Criminal Code* provide for a comprehensive federal statutory scheme that permits peace officers, acting through the Attorney General, to do precisely what the DRPS sought to do in this case. Accordingly, as a matter of law, s.487.01(1)(c) of the *Criminal Code* precluded the issuance of a general

warrant. Although resort to a general warrant to seize cryptocurrency may be available in some circumstances (e.g., where the cryptocurrency wallet is not hosted on an exchange such that there is no independent third party who can be compelled to restrain and control the asset)¹, it was not available where an independent third party is available to facilitate restraint and access. The procedure proposed by DRPS was thus substantively equivalent to the mechanism for preserving financial assets created by ss. 462.33 and 462.331 of the *Criminal Code*.

- 2) The Application Judge did not commit jurisdictional or legal error in refusing the general warrant on the basis that s.487.01(1)(c) was not satisfied. However, even if this Court were to conclude otherwise, the extraordinary remedies should not issue as the Application Judge also dismissed the application on the basis of findings that he made within the exercise of his jurisdiction that did not relate to questions of law alone:
 - a. First, the application judge was acting within the exercise of his jurisdiction in concluding that application materials did not establish reasonable grounds to believe that the proposed procedure would produce “information *concerning the offence*” as required by s.487.01(1)(a) of the *Criminal Code*. While *Amicus* agrees that “information” should be read broadly, it is limited by the qualification that the information must be about the offence. In the circumstances of this case, the Application Judge reasonably concluded that there was no basis to infer that transferring the cryptocurrency from the target wallets to a wallet controlled by the Durham Regional Police Service (“DRPS”) would tell police anything about the offence itself – about how it was committed, or who committed it.
 - b. Second, the application justice was acting within his discretion and jurisdiction when he concluded that it was not in the “best interests of justice” to grant the application as required under s.487.01(1)(b) of the *Criminal Code*. Where police seek a stand-alone order to take control of financial or other assets that are alleged to be proceeds of crime, Parliament has created a complete scheme in

¹ A general warrant thus may be available where the police propose to access the cryptocurrency through a suspect’s personal electronic device. See e.g. the Supplementary Affidavit of Taryn Snow [“Snow Supplementary Affidavit”], paras. 13a, 19(b) and (c), p. 6 [PDF] and [R. v. Vachon-Desjardins, 2022 ONCJ 43](#) at para. 7

Part XII.2 that creates important protections for those from whom the assets are to be seized. There are notice requirements *before* orders are made (ss. 462.33(5) and 462.331(5)), requirements that the Attorney General provide undertakings to safeguard the property (s. 462.33(7)), and mechanisms for individuals rendered indigent by the seizure to gain access to the funds for specified necessities (s. 462.34(4)(c)). These rigorous protections are absent from the ss. 489.1/490 scheme. Indeed, under s. 489.1(a), police may simply return the funds to the purported victim absent any meaningful judicial oversight.

II. FACTUAL CONTEXT

A. OVERVIEW

4. On March 7, 2023, the Crown in right of Ontario filed an application in the Ontario Court of Justice, prepared by D/C Taryn Snow of the DRPS, seeking a general warrant pursuant to s. 487.01 of the *Criminal Code* to seize cryptocurrency located in three “wallets” hosted on the cryptocurrency exchange Binance. D/C Snow deposed that she had reasonable grounds to believe that the specified cryptocurrency had originally been obtained from a Canadian resident through fraudulent means. The application also sought an assistance order pursuant to s. 487.02 directing Binance to facilitate the transfer of the specified cryptocurrency from the three target wallets into a secure wallet maintained by the DRPS. On March 20, 2023, Justice Burstein issued a written endorsement dismissing the application, on the basis that it did not satisfy any of the three prerequisites of s. 487.01: (1) it would not afford information concerning the offence; (2) there were other provisions authorizing the procedure or technique, namely a restraint order; and (3) issuing the warrant was not in the best interests of justice.

5. On May 12, 2023, the Attorney General of Ontario (“AGO”) filed an application seeking remedies in the nature of *certiorari* with *mandamus* in aid, asking this Court to quash the endorsement of Justice Burstein dismissing the general warrant application and to compel the

Ontario Court of Justice to issue the general warrant and assistance order. The AGO argues that the application judge committed jurisdictional error and erred in law.

B. THE INFORMATION TO OBTAIN

1) The Reasonable Grounds to Believe an Offence was Committed

6. In the Information to Obtain [“ITO”] the general warrant, D/C Snow outlined an alleged fraud committed against a Canadian complainant which was reported to police in late October 2021.² In late August 2021, the complainant was contacted by an individual purporting to be Brett Kissel, an American country singer that the complainant followed on a social media platform. This individual began chatting to the complainant over an instant messaging program and began to express romantic interest in the complainant. A week later, the suspect told the complainant that he had an investment opportunity in which the complainant could participate. The suspect initially directed the complainant to purchase \$2000 worth of Bitcoin, an online cryptocurrency, at a Bitcoin “ATM” and then to transfer the funds using an electronic QR code. As a result of further communications, the complainant ultimately purchased approximately \$65,000 worth of Bitcoin which he transferred via the QR code over the course of a number of transactions.

7. The complainant ultimately became suspicious after seeing pictures of his interlocutor’s left hand which lacked several distinguishing tattoos that Mr. Kissel had. His partner convinced the complainant to make a report to the DRPS.

8. The complainant continued to communicate with the suspects and advised them he wanted his money back. He was directed to a website that required login credentials provided by the

² The summary is taken from paragraph 50 of the *Certiorari* Application Record [“*Certiorari* AR”], Affidavit of Taryn Snow [“Snow Affidavit”], Exhibit A, Information to Obtain [“Snow ITO”]

suspect. When he entered the login information and attempted to complete the withdrawal, the screen froze. The complainant contacted the suspect again, and was directed to advance a further amount to “unfreeze” the bitcoin and send them to a different wallet address. The complainant did not provide the further advance.

9. There is little dispute that the facts set out by the affiant disclose reasonable grounds to believe the offences of fraud and possessions of the proceeds of crime were committed against JD.

2) The Investigation

10. Police obtained records of some of the transactions from the complainant.³ Using these records, police contacted the company that operated the ATM, obtaining a list of the wallet addresses in which the complainant had transferred the funds. The company was also able to advise that the funds originating from the complainant had subsequently been transferred to other wallet addresses, including four on the Binance cryptocurrency exchange.⁴

11. With the assistance of the RCMP’s cryptocurrency tracing software, DRPS tracked a portion of the BTC invested by JD into three cryptocurrency “wallets” hosted on the Binance exchange.⁵ Police learned that Binance was the largest global cryptocurrency trading platform, permitting users to trade in more than 600 different cryptocurrencies.

12. After being advised of the alleged fraud, Binance voluntarily froze these three wallets in December 2021. As of the timing of this application (approximately 16 months later) the owners

³ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, para. 55

⁴ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, para. 57

⁵ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 59-64. In its responding record, Binance compliance officer Molcsan-Spidel disputes the accuracy of this type of tracing.

of the wallets have never contacted Binance or the DRPS to inquire why their currency has been frozen.⁶ Binance confirmed that it would comply with a Canadian court order.⁷

13. DRPS subsequently obtained a production order on December 8, 2022 for the account information and transaction history of “several receiving addresses within Binance’s control”. Binance complied with the production order on December 13, 2022. The information obtained revealed the names of the account holders of the three target accounts and that each account-holder was located in Nigeria.⁸

3) The Grounds for a General Warrant

14. D/C Snow deposed that a general warrant was being sought “to authorize peace officers to seize the BTC cryptocurrency which was fraudulently obtained from the complainant”, which “would allow Binance to facilitate the transfer of 0.08022315 BTC from the above-referenced addresses to a secure wallet held by Durham Regional Police Service.”⁹ D/C Snow further explained that if the target cryptocurrency remained under Binance control during the investigation, there was a risk that it would be moved “to a cryptocurrency address not associated to Binance” as there “is no lawful order requiring the freeze to remain in place”.¹⁰

15. After detailing her grounds for believing that criminal offences had been committed by the target account-holders, whom D/C Snow described “as the primary suspects in my investigation”,¹¹ she addressed the remaining pre-conditions for the issuance of a general warrant. She did not believe there were other provisions available to her as it was her understanding that a

⁶ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 65-68, 70, pp. 38-44 [PDF]

⁷ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, para. 70b, p. 44 [PDF]

⁸ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 72-73, pp. 45-46 [PDF]

⁹ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 74-75, p. 46 [PDF]

¹⁰ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 77, p. 47 [PDF]

¹¹ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 86, p. 49 [PDF]

s. 487 search warrant was limited to seizure from specified places or receptacles and she did not believe that removing cryptocurrency from one wallet to another involved removal from a place or receptacle.¹²

16. D/C Snow dismissed the availability of a restraint order because she did not believe it “would adequately ensure against dissipation of the cryptocurrency”. It was her belief that restraint orders were “generally only effective when an individual stores their cryptocurrency through a reputable, Canadian service provider who will respect a Canadian court order.” Acknowledging that Binance had voluntarily frozen the accounts, and had indicated that it was prepared to comply with Canadian court orders, D/C Snow nonetheless deposed that she did not believe it was “safe to assume Binance will agree to freeze the cryptocurrency in its systems indefinitely.” As it operated “largely outside traditional financial regulatory regimes”, D/C Snow believed there existed “a substantial risk that Binance could unfreeze the cryptocurrency”.¹³ Moreover, while a Restraint Order would freeze the currency, it would not bring the currency under police control.

17. D/C Snow rejected the addition of a management order coupled with a restraint order as an appropriate substitute because her “intention is not to restrain the cryptocurrency for the purpose of management and ultimate forfeiture to His Majesty, but rather to investigate the alleged fraud, and, if appropriate return the cryptocurrency to its lawful owner pursuant to s. 489.1(1) and s. 490 of the Criminal Code.”¹⁴ Because forfeiture was conditional “on a successful domestic prosecution in relation to the subject property” and “it is not clear that will happen here”, D/C Snow expressed

¹² *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 88, pp. 49-50 [PDF]

¹³ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 89-90, pp. 50-51 [PDF]

¹⁴ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 91, p. 51 [PDF]

the believe that a combined restraint and management order would not be substantively equivalent to the proposed procedure.¹⁵

18. D/C Snow asserted that the issuance of the general warrant would be in the best interests of justice because it would “frustrat[e] the objective of the alleged fraud” and would “assist in gathering information of the criminal offence”.¹⁶ Despite stating that the seizure would be an “important investigative step”, D/C Snow did not explain what information could be gathered or how gathering it would advance the investigation beyond explaining that “here, there is something that police can do to respond to the fraud committed against the complainant.”¹⁷

C. THE PROPOSED ORDER

19. The joint general warrant and assistance order proposed by D/C Snow was brief, containing only two terms. First, Binance was directed to “facilitate the transfer of...the cryptocurrency...to a secure wallet held by the Durham Regional Police Service” through a two-step process. First, Binance would “send a small test amount of cryptocurrency” followed by the entire target amount once DRPS confirmed the initial transaction. Second, the proposed order stipulated a 14-day window of validity.¹⁸

D. THE APPLICATION JUDGE’S ENDORSEMENT

20. The Application Judge prepared and issued a written endorsement, explaining that he had “decided that this is one of those rare cases where it is necessary for me to provide reasons for dismissing the above-captioned application.”¹⁹ The Application Judge observed that the “target of

¹⁵ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 91, p. 51 [PDF]

¹⁶ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 94, pp. 51-52 [PDF]

¹⁷ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, paras. 95, p. 52 [PDF]

¹⁸ *Certiorari* AR, Snow Affidavit, Exhibit A, Snow ITO, pp. 90-91 [PDF]

¹⁹ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, para. 3

the orders being sought are [sic] a third party and not a suspect” and characterized the purpose of the application as “compelling the exchange to facilitate the recovery of some of the cryptocurrency transferred from the victim to the suspects...**not**...at gathering evidence relevant to the investigation or prosecution of the alleged perpetrators”.²⁰

21. The Application Judge accepted that the cryptocurrency held in the three target accounts was probably the proceeds of crime, but held that the other prerequisites of s. 487.01 were not satisfied. In particular, the Application Judge explained that there were a “variety of legal mechanisms” capable of authorizing the “recovery of property obtained by the commission of an offence” and in particular, the restraint provision in s. 462.33. The Application Judge expressed the view that the application before him “could likely have satisfied the statutory requirements for a restraining order under s. 462.33.”²¹ He rejected the affiant’s concern that Binance would not comply with a restraint order as speculative, determining that a “*Criminal Code* restraining order was a reasonable legal alternative to the general warrant sought in this case.”²²

22. The Application Judge concluded that it would additionally be “legally inappropriate to seek a general warrant for the purpose of seizing suspected proceeds of crime” as “it would stretch the intended meaning of Parliament’s use of the ‘information’ in s. 487.01...to extend the scope of general warrants to include the seizure of property for sole purpose of future compensation.”²³ The Application Judge also explained that granting the general warrant would “risk bringing the administration of justice into disrepute” because the proposed procedure might “amount to an abuse of the court’s process.”²⁴ In particular, the Application Judge expressed a concern that

²⁰ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, paras. 4, 6

²¹ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, paras. 9-10

²² *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, para. 12

²³ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, para. 13 [emphasis added]

²⁴ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, para. 14

“police have sought a general warrant for the purpose of taking money from the suspects so that the police may eventually give that money to the victim.” The Application Judge described this as an unlawful use of the general warrant provision.²⁵

E. THE SUPPLEMENTARY AFFIDAVIT OF D/C SNOW

23. As part of this application, D/C Snow prepared a supplementary affidavit in which she deposed that “in recent years, Canadian police have relied predominately [sic] upon general warrants to seize cryptocurrency identified as proceeds of crime.”²⁶ D/C Snow described a general warrant she had obtained in 2021 to obtain cryptocurrency held in a wallet, and identified a number of other investigations of which she was aware that had utilized a general warrant to seize cryptocurrency. As a result of her own personal knowledge and information she had gleaned from other police services through the use of an informal survey, D/C Snow listed ten other investigations in which police had obtained a general warrant to seize cryptocurrency.²⁷ In a number of these cases, the general warrant authorized police to seize the cryptocurrency by utilizing an electronic device seized from the suspect.²⁸ In at least four of the cases, the general warrant had also been directed toward the Binance exchange.²⁹

24. D/C Snow also disclosed a number of unsuccessful general warrant applications:

- a. On February 14, 2023, Robertson J. of the Alberta Provincial Court dismissed an application for a general warrant against Binance on the basis that the application did not explain how information concerning the offence would be obtained.

²⁵ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons of the Application Judge, para. 14

²⁶ Supplementary Affidavit of D/C Snow, para. 11

²⁷ Supplementary Affidavit of D/ C Snow, paras. 12-19

²⁸ Supplementary Affidavit of D/C Snow, paras. 13a, 19b, 19c,

²⁹ Supplementary Affidavit of D/C Snow, paras. 12, 13b, 19a, 19g

Robertson J. further noted that “it is not the purpose of s. 487.01 to return property where parties have suffered a loss because of an alleged offence”³⁰

- b. On April 14, 2023, Mulder J. of the British Columbia Provincial Court also rejected an application for a general warrant on the basis that he was not satisfied that “seizing the specified cryptocurrency and holding it in secure storage, leads to ‘information concerning the offence’”³¹
 - c. Lenehan J. of the Provincial Court rejected a general warrant application on the basis of jurisdictional concerns.³²
 - d. On June 2, 2023, Choy J. of the Provincial Court of Manitoba rejected a general warrant on the basis that the same mechanism was available through a restraint order under s. 462.33 or 490.8 of the *Criminal Code*, and that it was otherwise not in the best interests of justice to grant.³³
25. D/C Snow also included an endorsement from Tchir J. of the Alberta Provincial Court rejecting a search warrant to seize cryptocurrency. In the course of her endorsement rejecting the warrant, Tchir J. expressed the view that the proper avenue may be a general warrant relying on an article authored in the *Criminal Law Quarterly*.³⁴ In that article, the authors express the view that a general warrant may be available as it “seems likely that no other provision can authorize

³⁰ Supplementary Affidavit of D/C Snow, Exhibit A, p. 11 [PDF]

³¹ Supplementary Affidavit of D/C Snow, Exhibit A, p. 12 [PDF]

³² Supplementary Affidavit of D/C Snow, Exhibit A, p. 13 [PDF]

³³ Supplementary Affidavit of D/C Snow, Exhibit A, p. 14 [PDF]. While this is not yet in evidence, *amicus* inquired of the Crown about any restraint orders used to target cryptocurrency. Crown counsel advised that three days after the rejection of the general warrant by Choy J., police sought and obtained a restraint order against the property pursuant to s. 462.33. It is anticipated that this evidence will be the subject of a further affidavit.

³⁴ Supplementary Affidavit of D/C Snow, Exhibit B, pp. 17-18 [PDF]

the seizure of cryptocurrency”, since “there is no third party to whom notice is served and who would be responsible for executing the restraint.”³⁵ The authors do not address the existence of cryptocurrency exchanges such as Binance.

III. ISSUES AND THE LAW

A. THE GENERAL WARRANT PROVISION

26. Section 487.01 of the *Criminal Code* provides as follows:

487.01 (1) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person’s property if

(a) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;

(b) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and

(c) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.

27. This general warrant provision was introduced by Parliament in 1993 to fill any potential gaps in the availability of judicial authorizations to conduct searches and/or seizures. The provision “recognizes that Parliament cannot anticipate or imagine all investigative means or techniques that are or will become available to the police.”³⁶ Although the provision is broad and can capture almost any kind of investigative technique or procedure, general warrants are to play a “modest role” in the judicial authorization arsenal, “affording the police a constitutionally sound path for investigative techniques that Parliament” has not addressed and are properly construed as

³⁵ Jason Mitschele and Ira Glasner, “Taking the Cryptic out of Cryptocurrency Investigations”, 2020 68 C.L.Q. 85

³⁶ [R. v. Ha, 2009 ONCA 340](#) at para. 26

“rearguard warrants of limited resort, not frontline warrants of general application.”³⁷ General warrants should not be used presumptively so as to “prevent the circumvention of more specific or rigorous pre-authorization requirements for warrants”.³⁸

28. Police may nonetheless resort to a general warrant provided that the application satisfies four criteria:

- a. There are reasonable and probable grounds to believe an offence has been or will be committed;
- b. “Information concerning the offence” will be obtained through the search or seizure being requested;
- c. It is in the “best interests of the administration of justice” to grant the authorization; and
- d. There is “no other provision in this or any other Act of Parliament” that is available to obtain judicial approval for the investigative technique in issue.

29. A judge considering an application for a general warrant under s.487.01 has the discretion not to issue a warrant even where the statutory requirements are met.³⁹

B. THE AVAILABILITY OF CERTIORARI REVIEW

30. *Amicus* accepts that the weight of authority supports the AGO’s position that the extraordinary remedies of *certiorari* and *mandamus* are available to the Crown to review an application judge’s refusal to issue a general warrant.⁴⁰

³⁷ [R. v. Telus Communications Co., 2013 SCC 16](#) at para 91 to 93.

³⁸ [R. v. Telus Communications Co., 2013 SCC 16](#) at para 19 (Abella J. citing S. C. Hutchison et al., *Search and Seizure Law in Canada* (loose-leaf), at p. 16-40.3)

³⁹ [R. v. Duchcherer, 2006 BCCA 171](#)

⁴⁰ *textPlus Inc. (re)*, [2022] O.J. No. 4959 at paras. 38 – 48; [R. v. Brown, 2015 ABQB 728](#) at para. 40; [British Columbia \(Attorney General\) v. Brecknell, 2018 BCCA 5](#); [R. v. Brown, 2019 ONSC 5032](#)

31. However, the scope of that review is, as the AGO recognized, more difficult. As Watt J.A. has observed

“[j]urisdiction has to do with the authority to decide an issue or perform a duty, not the nature or correctness of the decision made...On subjects within its jurisdiction, if a court of limited jurisdiction misconstrues a statute or otherwise misdecides the law, the remedy to correct the legal error is an appeal from the final disposition, not an application for an order in lieu of the extraordinary remedies of mandamus or certiorari”⁴¹

32. In *R. v. Provincial Court of Saskatchewan*, the Queen’s Bench held that, since search warrants under s. 487 were discretionary in nature, “parties do not have access to *certiorari* review for an error of law – even one that finally disposes of a legal right”. Because the Justice of the Peace in that case only erred in law, Klatt J. dismissed the *certiorari* application.⁴² This decision is supported by the language of the Supreme Court in *R. v. Awashish*. There the Court rejected the proposition that *certiorari* “would be available to parties to correct errors of law on the face of the record”, citing the risk of “fragmenting trials, thereby introducing inefficiency, delay and the determination of issues on an incomplete record.”⁴³

33. The AGO argues that in the context of *ex parte* proceedings, the rationale underlying the wider *certiorari* review accorded to third parties, should apply. While there are some merits to the AGO’s argument, it must also be recognized that unlike third parties, the police or Attorneys General are not precluded from seeking further judicial authorizations as long as the fact of the first refusal is disclosed. In such cases, the state is granted a *de novo* hearing.⁴⁴ In that respect, therefore, the police are not placed in the same disadvantageous position by the error of law, since they are free to seek successive authorizations. That being said, *Amicus* recognizes that many of

⁴¹ [R. v. Vasarhelyi, 2011 ONCA 397](#) at para. 52

⁴² [R. v. Provincial Court of Saskatchewan, 2022 SKQB 184](#) at paras. 33-34

⁴³ [R. v. Awashish, 2018 SCC 45](#) at para. 17

⁴⁴ [R. v. Bond, 2021 ONCA 730](#) at paras. 30-35

the cases cited by the AGO seem inclined to grant *certiorari* remedies for both jurisdictional error and errors of law, and even to treat the two interchangeably at times.

C. THE APPLICANT’S CLAIMS OF JURISDICTIONAL & LEGAL ERROR

34. The AGO rests its claim of jurisdictional and legal error on the assertion that the trial judge misconstrued the ambit of the general warrant provision by concluding that seizing proceeds of crime in order to recompense victims lay outside the permissible boundaries of the general warrant. Three fundamental errors, the AGO says, underlie this purported jurisdictional error.⁴⁵ First, the Application Judge incorrectly concluded that seizure of proceeds of crime was not a legitimate purpose for an investigative warrant. Second, the Application Judge conflated the purpose of the proposed procedure with its substance, thus leading him to improperly apply an “investigate necessity” criterion in place of the “no other provision” requirement in s. 487.01(1)(c).⁴⁶ Third, the Application Judge came to the incorrect conclusion that other avenues to accomplish the police objective were legally available in the circumstances of this application.

35. The AGO submits that this alleged jurisdictional error subsequently infected the Application Judge’s assessment of whether the proposed procedure would supply information concerning the offence and whether it was in the best interests of justice.⁴⁷

36. Each argument is addressed in turn.

1) The Use of s. 487 and s. 487.01 Warrants to Seize Proceeds of Crime

37. The AGO points out that proceeds of crime are frequently seized during the execution of investigative warrants. That is undoubtedly true. *Amicus* does not read the Application Judge’s

⁴⁵ Applicant’s Factum, para. 60

⁴⁶ Applicant’s Factum, para. 64

⁴⁷ Applicant’s Factum, paras. 95, 106

endorsement to say otherwise. However, the rationale underlying the use of investigative search warrants to enter a physical premises and seize real property does not automatically justify the use of a general warrant for the stand-alone purpose of seizing possession of digital assets controlled by an independent third party. Read in the context of his reasons, the Application Judge was referring to “[u]se of the general warrant provision by the police to seize suspected fraudulently obtained cryptocurrency from an exchange company for future victim compensation” when he commented that he was “not satisfied that it would be legally appropriate to seek a general warrant for the purpose of seizing suspected proceeds of crime.”⁴⁸ The Application Judge was not, as the AGO suggests, holding that police could never use investigative warrants to seize proceeds of crime, but that they could not do so where the proposed procedure was entirely preservative in nature.

38. The Application Judge’s conclusion is well-supported by both practical and legal considerations, which introduce important distinctions between the seizure of moveable physical property and the stand-alone seizure of digital financial assets. In the case of moveable physical property such as banknotes for instance, the reality is that the property will often be in the direct control of the target(s) of the investigation. In most cases, police will be unable to confirm the exact location or amount of the currency except in the course of executing a search warrant.⁴⁹ A physical search is typically a necessary precursor to seizing moveable property.

39. Often this occurs while executing a search warrant under s. 487. But where the police investigation is coupled with other investigative techniques, such as the authority to execute

⁴⁸ *Certiorari* AR, Snow Affidavit, Exhibit B, Reasons for Decision, para. 13

⁴⁹ See e.g., [R. v. Hobeika, 2020 ONCA 750](#) at para. 23-24; [Ontario \(Attorney General\) v. 269 Weldrick Road West \(in rem\), 2020 ONSC 4605](#)

random traffic stops and perform vehicle searches,⁵⁰ or where police seek authorization to execute a covert search to verify the presence of contraband,⁵¹ or to delay a proposed search contingent on future events,⁵² police may also end up seizing property under the authority of a general warrant.

40. That does not mean that police can use a general warrant *whenever* they wish to seize proceeds of crime. Digital financial assets are not just different in form from physical moveable property such as cash but different in kind. Such assets are typically under the control of an independent third party, such as a bank. Police can take preparatory steps to ascertain the exact amount and source of the digital assets through the use of production orders served on the bank administering the target account, which in turn exists within a regulatory framework that imposes various obligations on the bank to comply with lawful requests made by law enforcement. In short, police can prospectively ascertain the assets which they wish to assume control over, and can use the auspices of the third party to facilitate that.

41. The electronic form of digital financial assets also has legal significance. As the affiant acknowledged, a s. 487 search warrant, by virtue of the requirement that the evidence sought “is in a building, receptacle or place” is restricted to the search for tangible objects.⁵³ In the context of the proceeds of crime provisions, the Supreme Court has observed a distinction between the nature of the property targeted by special warrants of seizure authorized by s. 462.32 and restraint orders authorized by s. 462.33: “While a special warrant of seizure deals with movable, tangible property such as vehicles and jewellery, a restraint order targets real estate, or intangible property

⁵⁰ See e.g. [R. v. Chanmany](#), 2013 ONSC 1937

⁵¹ See e.g. [R. v. Ford](#), 2008 BCCA 94 at paras. 50-51;

⁵² See e.g. [R. v. Jodoin](#), 2018 ONCA 638 at para. 18

⁵³ [R. v. Wong](#) (1987), 34 C.C.C. (3d) 51, 1987 CanLII 6858 (Ont. C.A.) at 61; [R. v. Lauda](#) (1998), 37 O.R. (3d) 513, 1998 CanLII 2776 (Ont. C.A.) (“A s. 487 search warrant is a standard investigative procedure which police officers have used for generations to enter premises to search for, and seize, tangible objects which they reasonably believe will provide evidence of the commission of a crime.”).

such as bank accounts.”⁵⁴ Parliament has explicitly recognized this distinction with the recent enactment of a special warrant provision authorizing police to search for digital assets using a computer program and to “seize – including by taking control of the right of access – the digital assets”.⁵⁵

42. The fact that police forces in the past few years, including DRPS, have successfully sought and obtained general warrants from judicial officers for the seizure of cryptocurrency does not establish that the police were correct to do so. It is clear that there is considerable uncertainty – even within the law enforcement community as the affiant acknowledges – as to the appropriate avenue for these types of seizure. As the affiant fairly deposes, a number of judicial officers in recent years have rejected police applications for a general warrant to seize cryptocurrency. In at least three cases, police subsequently successfully sought restraint orders.⁵⁶

43. The exact form in which the cryptocurrency is held may also be relevant here. In some of the cases cited by D/C Snow and discussed by the Applicant, the cryptocurrency was obtained through the suspect’s own device. It may be the case that in such a scenario, where the suspect has exclusive control of the account through his or her own electronic device, there is no mechanism outside of a general warrant to take control of that cryptocurrency. Indeed, this seems to be the premise upon which the authors of “Taking the Cryptic Out of Cryptocurrency Investigations”, cited by Tchir J. in support of the proposition that a general warrant may be the appropriate avenue for cryptocurrency seizures. The authors write⁵⁷:

⁵⁴ *Quebec (Attorney General) v. Larocche*, 2002 SCC 72 at para. 26

⁵⁵ *An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023, S.C. 2023, c 26*, s. 212, enacting s. 462.321 of the *Criminal Code*. At the time the Applicant’s factum was filed, this legislation had not been passed. It received royal assent on June 22, 2023 and is set to come into force 90 days from that date (s. 234).

⁵⁶ *Amicus* anticipates that this will be the subject of further affidavit evidence provided by D/C Snow or a designate.

⁵⁷ Jason Mitschele and Ira Glasner, “Taking the Cryptic out of Cryptocurrency Investigations”, 2020 68 C.L.Q. 85

By obtaining the private key, investigators have seized the *potential* to gain control of the cryptocurrency, but they have not seized the cryptocurrency itself. One cannot seize cryptocurrency without transferring the funds to a different wallet. Nobody has exclusive control over the funds when more than one person knows the private key. Without exclusive control, there is nothing the police can do to prevent someone else from transferring the money post-arrest.

Police may require a General Warrant under s. 487.01 of the *Criminal Code* ("the Code") in order to legally transfer the funds and seize cryptocurrency. A General Warrant is available where a particular investigative technique or procedure cannot properly be authorized by any other provision in the *Code* or any other federal statute.¹² It seems likely that no other provision can authorize the seizure of cryptocurrency.

Nor can such seizures be authorized by restraint orders under s. 462.33 of the *Code* or s. 14 of the *CDSA*. ***This is because there is no third party to whom notice is served and who would be responsible for executing the restraint.*** In fact, service of notice would have to go to the person investigated, and that person would be unlikely to cooperate and could move their assets upon service.

44. Where the cryptocurrency is held in a manner that mimics a traditional banking structure, on the other hand, such that an independent third party can exercise supervening control over the account, the Court must carefully consider whether there is any substantive difference between the directing that third party to facilitate the transfer of cryptocurrency, and obtaining a restraint and management orders that direct a bank to transfer control of some amount of currency to a designated individual. This point will be developed further below.

2) There are Other Legislative Regimes Governing the Proposed Procedure – s.487.01(1)(c)

45. As set out above, the core of the dispute before this Court is the availability of other provisions in the *Criminal Code* or in other Acts of Parliament which would authorize the police to seize the cryptocurrency. AGO argues that, in concluding that there were, the Application Judge committed jurisdictional error. Careful scrutiny of the proposed procedure, however, supports the Application Judge's conclusion that a restraint order under s. 462.33, coupled with a management

order under s. 462.331, is a legal mechanism available to police in these circumstances that is substantively equivalent to the procedure proposed by D/C Snow.

a. The Test in s. 487.01(1)(c) – Substantive Equivalence

46. When considering whether there is any other provision authorizing the proposed technique, procedure or thing to be done, the Court asks whether the technique or procedure proposed is “substantively different from what Parliament has already provided”⁵⁸ in other statutory provisions. The focus is not on the “formal trappings” of whether the investigative technique or procedure can be authorized in exactly the same way as police propose under the general warrant but on whether what is being requested is “substantively equivalent” to what can be authorized by another search and/or seizure provision. In his concurring reasons in *R. v. Telus*, Moldaver J.A. explained the substantive equivalent test as follows at paras. 77-81:

[77] *The test under s. 487.01(1)(c) must consider the investigative technique that the police seek to utilize with an eye to its actual substance and not merely its formal trappings.* The provision must be interpreted so as to afford the police the flexibility Parliament contemplated in creating the general warrant, while safeguarding against its misuse. As the facts of this case illustrate, there is a need for heightened judicial scrutiny where Parliament has provided an authorization for an investigative technique that is substantively equivalent to what the police seek but requires more onerous pre-conditions.

[78] In so concluding, I note that in creating the general warrant, Parliament did not erase every other search authorization from the Code and leave it to judges to devise general warrants on an ad hoc basis as they deem fit. *Courts must therefore be careful to fill a legislative lacuna only where Parliament has actually failed to anticipate a particular search authorization.* To do otherwise would chip away at the foundation that shapes the respective roles of the courts and Parliament in our system of criminal justice when individual rights and freedoms are at stake.

[79] That said, I recognize, as I must, that this approach accepts a measure of uncertainty by tasking judges with the job of inquiring into the substance of purportedly “new” investigative techniques. In my view, an interpretation that is faithful to the purpose of the “no other provision” requirement in s. 487.01(1)(c) necessarily demands as much. Two practical guidelines, however, should serve to mitigate concerns that may arise.

[80] First, it is important for the police to appreciate that general warrants are not warrants of general application. On the contrary, *they are to be used sparingly, when the investigative technique they wish to employ is truly different in substance from an investigative technique*

⁵⁸ *R. v. Telus Communications Co.*, 2013 SCC 16 – Moldaver J. at para 100 and 102

accounted for by another legislative provision. Where uncertainty exists, the police would do well to err on the side of caution. They must know — with certainty — that general warrants may not be used as a means to circumvent other authorization provisions that are available but contain more onerous preconditions.

[81] Second, ***when judges are faced with an application for a general warrant where the investigative technique, though not identical, comes close in substance to an investigative technique covered by another provision for which more rigorous standards apply, they should proceed with extra caution.*** At a minimum, judges should look closely at the material filed and satisfy themselves that the request for a general warrant is genuine and not merely a device to escape the rigours of another authorization provision. Where careful scrutiny establishes that a proposed investigative technique, although similar, has substantive differences from an existing technique — not simply that it is similar in substance but different in form — judges may grant the general warrant, but they should be mindful of their obligation under s. 487.01(3) to impose terms and conditions that reflect the nature of the privacy interest at stake. In doing so, they may borrow as appropriate from the conditions that Parliament has chosen to impose on the substantively similar existing authorization.

47. An example of the improper circumvention of another authorization provision through the use of a general warrant is illustrated in *R. v. Christiansen*. The police suspected that the Appellant was utilizing a storage unit as a stash house. They sought, and obtained, a general warrant to enter the stash house for the purpose of determining whether there were controlled substances inside. When they entered, they documented the controlled substances and applied for a search warrant to seize the same. The accused was charged and convicted. On appeal, the Court concluded that the general warrant was wrongly issued⁵⁹:

[11] In this case, the general warrant was issued, in substance, for the same investigative technique available under *CDSA*, s. 11, namely, to search the Unit. The police could not satisfy the requirements for a search under *CDSA*, s. 11 because they did not have reasonable and probable grounds to believe there was evidence at the Unit. In effect, the police used the general warrant for the impermissible purpose of circumventing the standards required for obtaining a *CDSA* s. 11 warrant.

48. Before this Court can determine whether the DRPS application satisfies s. 487.01(1)(c) it must accurately characterize what the proposed procedure is trying to do. As the AGO correctly points out, the proposed technique, procedure or thing to be done must not be conflated with its investigative aim. The availability of different avenues to arrive at a particular investigative goal

⁵⁹ [*R. v. Christiansen*, 2017 ONCA 941](#) at para. 11

does not preclude resort to a general warrant.⁶⁰ Conversely, however, the proposed procedure must not be construed so narrowly so as to disguise the substantive similarity by over-reliance on formal distinctions.

49. Applying this to the present case, the primary aim of the DRPS is to restore some part of the complainant's fraudulently dissipated property. The mechanism proposed by the police to accomplish this is an authorization to "seize" the target cryptocurrency from the three target wallets, coupled with an assistance order directing Binance to facilitate the seizure by transferring the target cryptocurrency from the three wallets into a wallet held by DRPS. As D/C/ Snow explained in her ITO:

74) As set out above and in the attached draft order, I am requesting a general warrant pursuant to section 487.01 of the *Criminal Code*, that would authorize peace officers to seize the BTC cryptocurrency which was fraudulently obtained from the complainant and is located in the following frozen addresses held on the Binance exchange:

75) The general warrant would allow Binance to facilitate the transfer of 0.08022315 BTC from the above-referenced addresses to a secure wallet held by the Durham Regional Police Service. This is the amount of the complainant's cryptocurrency that is associated with the alleged fraud and is now located across all three target addresses.

50. The question that this Court must consider therefore is whether there is any other statutory provision enacted by Parliament that would provide a mechanism for substantially the same technique, procedure or thing being requested. If the answer is yes, then a general warrant is not available. As is set out below, *Amicus* takes the position that the restraint and management regime does provide a substantively similar mechanism.

⁶⁰ [R. v. Ha, 2009 ONCA 340](#) at para. 43

b. Restraint & Management Orders⁶¹ are Substantively Similar to the Proposed Procedure

51. In 1989, Parliament created a special regime governing proceeds of crime “for the purpose of combatting enterprise crime and drug trafficking” found in Part XII.2 of the *Criminal Code*.⁶² By targeting the proceeds of crime rather than the offender, the legislation created “enforcement techniques that enable the police to freeze or immobilize the property of criminal organizations regardless of whose possession it may be in, even before charges are laid.”⁶³ The purpose of the legislation is therefore prospective in nature, aimed at preserving property. However, it also has an investigative dimension; as the Supreme Court has recognized, Part XII.2 is also designed to “facilitate criminal investigations, by enacting procedural provisions that make property, and information about it, more readily accessible to the police and the Crown.”⁶⁴ Restraint and management orders in particular target “intangible property such as bank accounts”.⁶⁵

52. A restraint order, which prohibits “any person from disposing of, or otherwise dealing with any interest in, the property specified in the order” is available on application by the Attorney General which satisfies a judge that there are reasonable grounds to believe “that there exists...any property in respect of which an order of forfeiture may be made under subsection 462.37(1) or (2.01) or 462.38(2) in respect of a designated offence”. Restraint orders have extraterritorial jurisdiction, including outside of Canada, by virtue of s. 462.33(3.1).

⁶¹ While the analysis below focuses on restraint and management orders in relation to proceeds of crime, it is important to acknowledge that restraint and management orders are also available for “offence-related property” by virtue of s. 490.8. Thus, in circumstances other than the case at bar, where police are not satisfied that the property is proceeds of crime, but that it is being used to facilitate an offence (e.g. to purchase drugs or firearms), a similar regime is available.

⁶² [*Quebec \(Attorney General\) v. Laroche*, 2002 SCC 72](#) at para. 23

⁶³ [*Quebec \(Attorney General\) v. Laroche*, 2002 SCC 72](#) at para. 25

⁶⁴ [*Quebec \(Attorney General\) v. Laroche*, 2002 SCC 72](#) at para. 26

⁶⁵ [*Quebec \(Attorney General\) v. Laroche*, 2002 SCC 72](#) at para. 26

53. In turn, the Attorney General can apply for a management order under s. 462.331, appointing any person “to take control of and to manage or otherwise deal with all or part of the property”. A management order can also be used to “require any person having possession of that property to give possession...to the [appointed] person” (s. 462.331(1)(b)). The appointed manager has the power to sell the property where it is rapidly depreciating, destroy the property where it has little or no value, or have it forfeited to the government “to be disposed of or otherwise dealt with in accordance with the law”. In the latter case, the property (other than real property or a conveyance) will be forfeited if, on application to the court and notice being published, no one asserts an interest in the property in the course of the 60-day notice period.

54. It is the position of *Amicus* that there is little differentiating the situation facing the DRPS in this case from the situation where police wish to preserve alleged proceeds of crime that they trace to a particular bank account administered by a traditional bank with a physical presence in Canada. There can be no dispute that, if police wished to take control of the money held in a particular bank account, with a view to preserving it for potential restitution to the victim of a crime, they would not be able to avail themselves of the general warrant provision in light of the existence of the mechanisms in Part XXII.2, which were specifically designed to facilitate this sort of seizure.

55. Just as with bank accounts, where control is shared by the owner of the bank account, and it is the third-party banking institution that administers, maintains and guarantees the account, here access to the digital wallet is shared between the holder of the private key and the exchange, Binance, which administers and maintains the account. Technological particulars aside, holding a wallet on Binance is practically no different than maintaining a bank account at a traditional bank. In both cases, police seeking to seize the assets in either the wallet or the bank account rely on the

cooperation of the institutional third party to facilitate access to and control over the digital assets. As will be developed below, the distinction between a “seizure” versus “restraint and management” in these circumstances is one of terminology, not substance. At the heart of both situations, what the police seek is a court order compelling the institutional third party to facilitate the transfer of funds from the target account/wallet to an account/wallet managed by the DRPS. As a result, the Application Judge did not err or exceed his jurisdiction in concluding that there were other substantively similar statutory provisions available to police.

c. The Arguments of the Applicant to the Contrary

56. The AGO argues that restraint and management orders were not substantively similar to what DRPS sought because such orders were not available to the DRPS in the present case as there were no reasonable grounds to believe that the target cryptocurrency may be forfeited under either s. 462.37(1) or 462.38(2), both of which require the institution of a prosecution. As a preliminary point, the fact that police cannot satisfy the preconditions for an authorization does not entail that the resort to a general warrant constitutes a different legal mechanism. For example, s.184.2(2) authorizes a peace officer to apply for a one-party consent wiretap authorization before a provincial court judge but only in respect of offences listed in s.183 of the *Criminal Code*. Disobeying a court order contrary to s.127 of the *Code* is not a designated offence. Therefore, a peace officer cannot apply for a one-party consent authorization in order to investigate such an offence. That would not in turn provide a basis for the peace officer to apply to do the same thing by way of a general warrant.

57. As Moldaver J. held in *Telus*, “there is a need for heightened judicial scrutiny where Parliament has provided an authorization for an investigative technique that is substantively

equivalent to what the police seek but requires more onerous pre-conditions.” Reasonable grounds to believe that the target cryptocurrency may be the subject of a forfeiture order is a more onerous pre-condition than anything in s. 487.01. Permitting the DRPS to resort to the general warrant as a result of its inability to satisfy the criteria for s. 462.33 would be the very mischief that the Supreme Court sought to guard against in *Telus* when Abella J. cautioned that “s. 487.01(1)(c) should be broadly construed to ensure that the general warrant is not used presumptively. This is to prevent the circumvention of more specific or rigorous pre-authorization requirements for warrants.”⁶⁶

58. In any event, the AGO would not have been precluded from obtaining a restraint and management order in this case. In *Quebec v. Laroche*, the Supreme Court explained that a judge entertaining an application for a restraint order “must attempt to forecast the future. He or she must determine, on a balance of probabilities, whether an order of forfeiture would be made under either of ss. 462.37(1) and 462.38(2)”⁶⁷ This provision can be interpreted in one of two ways. It could be interpreted conditionally – if a prosecution were instituted, are there reasonable and probable grounds to believe that a forfeiture under either provision would occur. This interpretation is consistent with the prospective nature of Part XII.2. It could, however, also be interpreted to require the AG to establish that there are reasonable and probable grounds to believe that a prosecution will occur and that an order of forfeiture “would eventually be made according to the applicable standards of proof.”⁶⁸ It is the latter interpretation the AGO adopts.

⁶⁶ [R. v. Telus Communications Co., 2013 SCC 16](#) at para. 18

⁶⁷ [Quebec \(Attorney General\) v. Laroche, 2002 SCC 72](#) at para. 37

⁶⁸ [Quebec \(Attorney General\) v. Laroche, 2002 SCC 72](#) at para. 39

59. This Court does not have to resolve this interpretive issue, however, because even if the stricter interpretation were correct, it is not clear that the DRPS could not have satisfied that threshold. Section 462.38 permits the AG to apply for forfeiture where: (a) an Information has been laid in respect of the designated offence; (b) it can establish beyond a reasonable doubt that the property is proceeds of crime; (c) the property was obtained through the commission of the designated offence which was the charge alleged; and (d) the accused has died or absconded. For the purposes of subsection (d), an accused will be deemed to have absconded if “in the case of a person who is not or never was in Canada, the person cannot be brought within that period to the jurisdiction in which the warrant or summons was issued” within six months. In this case, police were aware of the names of the wallet-holders through the production order. D/C Snow identified these individuals as suspects. There were arguably reasonable grounds to believe that police could have laid an Information charging those men with fraud and proceeds of crime and then applied to forfeit the restrained and managed funds after six months.

60. The remaining barriers relied on by the AGO similarly do not establish that the restraint and management regime is substantively different than the proposed procedure. The AGO’s argument that, because only the AG can apply for restraint and management orders, the police are frustrated in their ability to advance an investigation is misplaced. This submission first ignores the practical reality that, in the course of an ongoing investigation, the Attorney General does not act independently from the police. It is the police, in their capacity as investigators, who alert the Crown to the existence of potential proceeds to be restrained and managed, and who coordinate the application with the Crown. While the Crown, representing the Attorney General, must oversee and submit the application, it is typically a police officer who has been intimately involved in the

ongoing investigation that swears the Information to Obtain in support of the restraint and management orders, just as the officer-in-charge did in this case.⁶⁹

61. The fallacy of the argument is further demonstrated by considering the following example where the police want to obtain evidence of a conspiracy by accessing private communications. If the communications have already happened, a police officer can apply for a search warrant to search an electronic device under s.487 of the *Criminal Code*. If the communications have happened and reside on a telecommunication server, they can request a production order for the third party to produce those messages. If a peace officer wants to intercept communications in real time or prospectively, there is no specific statutory mechanism available to a regular peace officer to seek judicial authorization to do the same. It is only a designated agent of the Attorney General (a Crown agent) that can apply under s.185 of the *Criminal Code* for a Part VI wiretap authorization. In Ontario, the Crown agent is normally an Assistant Crown Attorney or Public Prosecutor designated for that purpose. On the Attorney General's argument, a regular peace officer who cannot apply for a Part VI authorization would therefore be able to apply for a general warrant under s.487.01 of the *Criminal Code* to intercept the real time or prospective communications.

62. Additionally, the purposive distinction between the proceeds of crime restraint and management regime and the proposed procedure is nowhere near as stark as the AGO suggests. As noted above, the Supreme Court has recognized that there is an investigative component to Part XII.2. More importantly for the present case, however, it is clear from D/C Snow's ITO that her primary purpose was not to advance the investigation, but to preserve the potential proceeds with

⁶⁹ Of note, it appears that counsel for the Applicant reviewed the application package and submitted it on behalf of police: *Certiorari* AR, Snow Affidavit, Exhibit A, p. 11 [PDF]

a view to making restitution to the complainant. This is evident throughout her ITO. For instance, D/C Snow expresses concern that the restraint order would “not adequately ensure against dissipation of the cryptocurrency” and that “notice requirements and legal assistance treaties may operate too slowly to effectively freeze the cryptocurrency prior to its disposition or transfer”⁷⁰. To the extent that D/C Snow articulates an investigative purpose for the proposed procedure that is distinct from preventing the dissipation of the cryptocurrency, this was evidently a secondary concern.

63. Nor can the two mechanisms be differentiated by their procedural complexity. Contrary to the AGO’s contention,⁷¹ both the proposed procedure and the restraint/management orders require two separate orders. The affiant here sought both a general warrant and an assistance order under s. 487.02. Similarly, just as the affiant did in the application at bar, there is nothing preventing the Attorney General from seeking a restraint order and a management order by means of an omnibus application. Indeed, Attorneys General commonly proceed in this manner.⁷² Although the AGO claims not to want to manage the target cryptocurrency, that is exactly what the affiant proposes to do by taking control in order to preserve it from dissipation. Unless the AGO takes the position that there is no dispute as to the complainant’s lawful entitlement to the cryptocurrency,⁷³ such that the DRPS would be justified in immediately returning the cryptocurrency to the complainant

⁷⁰ *Certiorari* AR, Snow Affidavit, Exhibit A, ITO, para. 89, p. 50 [PDF]

⁷¹ Applicant’s Factum, paras. 81

⁷² See e.g. [R. v. Am-Stat Corporation, 2011 ONSC 7462](#) at para. 8 (in the context of restraint and management orders for offence-related property pursuant to ss. 490.8 and 490.81); [R. v. Nguyen, 2013 ONSC 6913](#) at para. 19; [R. v. Murtaza and Murtaza, 2011 ONSC 7577](#) at para. 3; [Canada \(Attorney General\) v. Sjoquist, 2014 SKQB 66](#) at paras. 1-2

⁷³ The issues raised by the Respondent suggest that the complainant’s lawful entitlement to the cryptocurrency currently in the target accounts is not beyond dispute.

pursuant to s. 489.1(1)(a), the DRPS will necessarily be required to manage the proceeds while the issue of lawful detention is determined.

64. Finally, the AGO argues that the restraint and management order is impractical because it requires the ongoing cooperation of Binance. Setting aside the Application Judge's non-reviewable factual determination that this concern was speculative, the use of a management order directing the transfer of the target cryptocurrency to the DRPS wallet, which is exactly what DRPS hopes to achieve through the general warrant and assistance order, is a complete answer to that issue. Once the cryptocurrency is in the DRPS wallet, Binance's ongoing cooperation is no longer required. All that is required is initial compliance with the restraint and management order. Binance has appeared on this application and has indicated a willingness to comply with any court order.

3) The Proposed Procedure Will Not Furnish "Information Concerning the Offence" – s.487.01(1)(a)

65. Even if the Court is of the view that a restraint and management order is not substantively similar to the proposed procedure, and that the Application Judge committed jurisdictional error in concluding so, the Application Judge's finding that the application did not satisfy the "information concerning the offence" criterion is an exercise of discretion that is immune from prerogative review, even if this Court might view the sufficiency of the application material differently. The Application Judge's conclusion is supported by the record on the application below.

66. When a warrant is requested under s.487.01 of the Criminal Code, the judge must be satisfied that there are reasonable grounds to believe that the "information concerning the offence

will be obtained” through the use of the procedure under s.487.01(1)(a).⁷⁴ Further, there must be grounds to believe that the information related to the specified offence(s) will be present at the time of the execution of the warrant.⁷⁵

67. The language “information concerning the offence” in s.487.01(1)(a) is different than “will afford evidence with respect to the commission of an offence” used in s.487 of the *Criminal Code*. Section 487.01(1)(a) is “a broad statement, encompassing all materials which might shed light on the circumstances of an event”. “The natural and ordinary meaning of this phrase is that anything relevant or rationally connected to the incident under investigation, the parties involved and their potential culpability falls within the scope of the warrant.”⁷⁶ Section 487.01 authorizes more than a search or seizure of “evidence”. In that sense, the use of the word “information” is broader.⁷⁷

68. There is a dearth of jurisprudence on the question of what amounts to “information concerning the offence” to satisfy this criterion. In *R. v. Ongley*, Langdon J. in a pre-*Telus* case concluded that a general warrant was available post-conviction to permit the Crown to gather “information” about an offender relevant to sentencing and, in particular, a potential dangerous offender/long-term offender proceeding. Langdon J. suggested that the phrase “includes whatever is necessary to get at the truth and properly and fairly dispose of the case.”⁷⁸

69. However, “information” cannot be so broadly construed as to capture anything that the police want to do in connection with an investigation. For example, in *R. v. Wise*, Lacelle J. concluded, for various reasons, that a general warrant should not have issued to permit the police

⁷⁴ [R. v. Lucas 2014 ONCA 561](#) at para. 113

⁷⁵ [R. v. Lucas 2014 ONCA 561](#) at para 115.

⁷⁶ [CanadianOxy Ltd. v. Canada \(A.G.\) \[1999\] 1 SCR 743](#) at para 15.

⁷⁷ *R. v. Ongley* [2003] O.J. No. 3934 (SCJ) at para 9 referred to in [R. v. Wise 2020 ONSC 7716](#) at para 87 without comment.

⁷⁸ *R. v. Ongley* [2003] O.J. No. 3934 (SCJ)

to covertly search the accused's residence. In doing so, the court rejected the Crown suggestion "information" was broad enough to contemplate authorizing a surreptitious entry into the residence of a murder suspect to confirm that nothing of interest was present because "even the absence of information would be 'information' that could meet the requirements of s.487.01 of the *Criminal Code*."⁷⁹

70. In *In the matter of an application for a General Warrant pursuant to section 487.01 of the Criminal Code of Canada, R.S.C. 1985*,⁸⁰ a judge was asked to grant a general warrant to obtain information about a medical facility patient's status. The police had grounds to arrest the patient but did not want to do so in the medical facility where the patient was being treated. Instead, they wanted to be kept apprised of the patient's health by compelling the facility to relay this information to them including information as to whether the patient left the facility or was going to be discharged. In denying the warrant, the judge concluded that there was no investigative technique or procedure engaged but more importantly, a general warrant can only be issued if the judge is satisfied that there are reasonable grounds to believe that issuing the warrant will result in "information" concerning the offence being obtained. Nowhere in the information to obtain did the affiant indicate that any such information will be obtained as a result of the issuing of the general warrant requested in relation to the offences allegedly committed by the patient or in relation to any which might be committed.

71. In this case, the application placed before the Application Judge was almost wholly silent on the issue of what information the police hoped to glean by seizing the funds. As pointed out

⁷⁹ [R. v. Wise, 2020 ONSC 7716](#) at para. 110

⁸⁰ [In the matter of an application for a General Warrant pursuant to section 487.01 of the Criminal Code of Canada, R.S.C. 1985, 2018 CanLII 39387](#) (NLPC)

above, the Application Judge's determination that the record did not disclose any grounds to believe information concerning the offence would be obtained is an exercise of his discretion, not a basis for *certiorari* review.

72. On this certiorari application, however, the AGO now argues that there are three types of information that the proposed procedure could produce. First, the AGO argues that the mere fact that cryptocurrency is data satisfies the information requirement. While computer data may constitute information, it is difficult to understand how this constitutes information about the offence. Second, the AGO speculates that the seizure of the cryptocurrency may stimulate conversation or even a claim to DRPS by the holders of the wallet. In the abstract, this may provide a basis in some investigations, but here the record discloses that in the year and a half during which the funds have been frozen by Binance, the owners have made no claim. There is no reasonable inference that the seizure would stimulate what the freeze did not. Finally, the AGO argues that the fact of the transfer itself would somehow provide information about the offence. This is inaccurate. All the transfer could confirm is that the Binance records, obtained through the production order, are accurate. It says nothing about the source of the cryptocurrency or the alleged fraud. Any reasoning to the contrary rests on the circular premise that because the funds were transferred on the basis that there is reason to believe that they are proceeds of crime, this yields information confirming that they are the proceeds of crime.

4) Authorizing the Proposed Procedure by Means of a General Warrant is not in the Best Interests of Justice – s.487.01(1)(b)

73. Even more so than the question of whether the propose procedure would produce information concerning the offence, an Application Judge's conclusion as to whether the issuance of a warrant is in the best interests of justice is clearly a discretionary one taken in the exercise of

his or her jurisdiction. It is difficult to articulate circumstances in which prerogative review could issue on such a basis, even where the Application Judge's decision rested on an error in law. But as with the information criterion, the Application Judge's conclusion was reasonable and open to him on the record.

74. The “best interests” criterion is intended to prevent the misuse of the general warrant provision without “swallowing the distinct analytical question that the ‘no other provision’ test asks.”⁸¹ It requires a balancing of the proposed intrusion on privacy against the law enforcement goal to find evidence. It also considers how the investigation will be advanced if the general warrant is granted or not granted.⁸² From a principled perspective, there is no reason why a Court could not also consider whether there are other means, short of the use of a general warrant, to accomplish the investigative goal even if there is no other substantially similar provision that would authorize the particular investigative technique or procedure being sought.

75. Even if the general warrant authorization could be substantively distinguished from the restraint and management regime, it is a relevant consideration under this criterion that that regime would still be available to police. Importantly, under this criterion, the restraint and management regime provides a number of important protections for those from whom the property is seized that are absent in the provisions of s. 489.1 and 490. First, one of the pre-conditions for a restraint order is that the Attorney General is required to provide undertakings “as the judge considers appropriate with respect to the payment of damages or costs” (s. 462.33(7)). Second, s. 462.33(5) requires notice to be given to any interested party prior to the any order being made unless the

⁸¹ [R. v. Telus 2013 SCC 16](#) at para 96 per Moldaver J.

⁸² [R. v. Finlay and Grellette 1985 CanLII 117 \(ONCA\)](#); N. Hassan, M. Lai, D. Schermbrucker, and R. Schwartz “Search and Seizure” (Edmonds, 2021) at p.214

judge determines that the provision of such notice could lead to the dissipation of the property. Third, s. 462.34 provides a mechanism for those from whom the property has been seized to access the property for certain basic necessities, including reasonable living expenses and business and legal expenses. The regime thus ensures a robust protection for funds seized as the proceeds of crime, as the DRPS wishes to do in this case.

76. By comparison, ss. 489.1 and 490 do not offer the same degree of protection. Indeed, as the AGO acknowledges in its factum, seized property that is subject to that disposition regime may be returned even without any meaningful judicial oversight. Section 489.1(1)(a) permits a police officer, in the exercise of his or her own discretion as to whether there is any “dispute” about, to simply return the property to the person the officer considers to be the lawful owner, before it is even brought before a justice. There is no meaningful review of this discretion. At this stage of the process, a justice has “limited discretion”.⁸³ As Ratushny J. held in *R. v. Kawecki*, s. 490(1), which provides for the justice to make an order disposing of any items brought before him or her, does not “allow for the holding of a hearing by the justice of the peace as to the merits of the evidence from the peace officer that the thing seized should be detained or returned.”⁸⁴ Ratushny J. rejected the notion that ss. 489.1 and 490 “protect the proprietary rights of the innocent person” at this stage; rather the purpose of this aspect of the scheme is simply “to mandate how a peace officer acting in the execution of his duties is to decide on restitution or detention of the thing seized.”⁸⁵

77. Where police can accomplish the exact same aim with increased protection for the rights of the persons from whom the property was seized, the best interests of justice weigh in favour of

⁸³ [R. v. Bellinger, 2017 ONSC 1639](#) at para.33

⁸⁴ [R. v. Kawecki, 2014 ONSC 3584](#) at para. 35

⁸⁵ [R. v. Kawecki, 2014 ONSC 3584](#) at para. 37

dismissing the application for a general warrant. The Application Judge recognized this and his decision on this point is a matter of discretion that implicates neither an error of law, nor a question of jurisdiction.

D. CONCLUSION

78. The legal question of broad application posed by this prerogative review – whether the seizure of cryptocurrency from a third party exchange can be authorized through resort to the general warrant provision – should be answered in the negative. In such circumstances, the restraint and management provisions of the proceeds of crime legislation (or s. 490.8 in the appropriate circumstances) provide a substantively similar mechanism that precludes the use of the general warrant.

79. In any event, the Application Judge refused the general warrant and assistance order not only because it did not comply with s. 487.01(1)(c), but because it did not satisfy the other criteria of reasonable grounds to believe it would supply information concerning the offence, and being in the best interests of justice. These were reasonable exercises of the Application Judge’s discretion. In the event that this Court is of the view that the Application Judge did commit jurisdictional error with respect to s. 487.01(1)(c), then the appropriate remedy is to correct that error, but dismiss the application for *certiorari* with *mandamus* in aid. The DRPS would then be entitled to re-apply for a general warrant in the Ontario Court of Justice.

July 28, 2023

ALL OF WHICH IS RESPECTFULLY SUBMITTED



Michael W. Lacy
Amicus Curiae



Bryan Badali
Amicus Curiae

IV. LIST OF AUTHORITIES

Case Law

1. [R. v. Vachon-Desjardins, 2022 ONCJ 43](#)
2. [R. v. Ha, 2009 ONCA 340](#)
3. [R. v. Telus Communications Co., 2013 SCC 16](#)
4. [R. v. Duchcherer, 2006 BCCA 171](#)
5. textPlus Inc. (re), [2022] O.J. No. 4959
6. [R. v. Brown, 2015 ABQB 728](#)
7. [British Columbia \(Attorney General\) v. Brecknell, 2018 BCCA 5](#)
8. [R. v. Brown, 2019 ONSC 5032](#)
9. [R. v. Vasarhelyi, 2011 ONCA 397](#)
10. [R. v. Provincial Court of Saskatchewan, 2022 SKQB 184](#)
11. [R. v. Awashish, 2018 SCC 45](#)
12. [R. v. Bond, 2021 ONCA 730](#)
13. [R. v. Hobeika, 2020 ONCA 750](#)
14. [Ontario \(Attorney General\) v. 269 Weldrick Road West \(in rem\), 2020 ONSC 4605](#)
15. [R. v. Chanmany, 2013 ONSC 1937](#)
16. [R. v. Ford, 2008 BCCA 94](#)
17. [R. v. Jodoin, 2018 ONCA 638](#)
18. [R. v. Wong \(1987\), 34 C.C.C. \(3d\) 51, 1987 CanLII 6858 \(Ont. C.A.\)](#)
19. [R. v. Lauda \(1998\), 37 O.R. \(3d\) 513, 1998 CanLII 2776 \(Ont. C.A.\)](#)
20. [Quebec \(Attorney General\) v. Laroche, 2002 SCC 72](#)
21. [R. v. Christiansen, 2017 ONCA 941](#)
22. [R. v. Am-Stat Corporation, 2011 ONSC 7462](#)
23. [R. v. Nguyen, 2013 ONSC 6913](#)
24. [R. v. Murtaza and Murtaza, 2011 ONSC 7577](#)
25. [Canada \(Attorney General\) v. Sjoquist, 2014 SKQB 66](#)
26. [R. v. Lucas 2014 ONCA 561](#)
27. [CanadianOxy Ltd. v. Canada \(A.G.\) \[1999\] 1 SCR 743](#)
28. *R. v. Ongley* [2003] O.J. No. 3934 (SCJ)

29. [*R. v. Wise* 2020 ONSC 7716](#)
30. [*In the matter of an application for a General Warrant pursuant to section 487.01 of the Criminal Code of Canada, R.S.C. 1985*, 2018 CanLII 39387 \(NLPC\)](#)
31. [*R. v. Finlay and Grellette* 1985 CanLII 117 \(ONCA\)](#)
32. [*R. v. Bellinger*, 2017 ONSC 1639](#)
33. [*R. v. Kawecki*, 2014 ONSC 3584](#)

Legislation

1. [*An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023, S.C. 2023, c 26*](#)

Commentary

1. Jason Mitschele and Ira Glasner, “Taking the Cryptic out of Cryptocurrency Investigations”, 2020 68 C.L.Q. 85
2. N. Hassan, M. Lai, D. Schermbrucker, and R. Schwartz “Search and Seizure” (Edmonds, 2021) at p.214

ONTARIO
SUPERIOR COURT OF JUSTICE
(Central East Region)

IN THE MATTER OF an order dismissing an application for a general warrant sought by the Durham Regional Police Service pursuant to section 487.01 of the *Criminal Code*;

AND IN THE MATTER OF an order dismissing an application for an assistance order sought by the Durham Regional Police Service pursuant to section 487.02 of the *Criminal Code*;

AND IN THE MATTER OF an application by the Attorney General for Ontario for an order in the nature of *certiorari* with *mandamus* in aid to quash the above-referenced orders and compelling the Provincial Court to exercise its jurisdiction to grant the general warrant and assistance order.

FACTUM OF AMICUS CURIAE

BRAUTI THORNING LLP
2900 – 161 Bay St.
Toronto, ON M5J 2S1

Michael W. Lacy
Tel: (416) 360-2776
mlacy@btlegal.ca

Bryan Badali
Tel: (416) 360-2777
bbadali@btlegal.ca

Amicus Curiae



Law Society
of Ontario

Barreau
de l'Ontario

TAB 1

Anti-Money Laundering: Protecting Your Litigation Practice

Cryptocurrency Considerations

PowerPoint

Michael Fawcett, Crown Law Office – Criminal
Ministry of the Attorney General

Fredrick Schumann
Stockwoods LLP

Evan Thomas
Wealthsimple

October 17, 2023



Cryptocurrency Considerations

Anti-Money Laundering: Protecting Your Litigation Practice

October 17, 2023

Michael Fawcett, *Crown Law Office – Criminal, Ministry of the Attorney General*

Fredrick Schumann, *Stockwoods LLP*

Evan Thomas, *Wealthsimple*

Cryptocurrency and Your Litigation Practice

- Cryptocurrency has been at issue in many types of cases:
 - Criminal, commercial, family, insolvency, civil fraud, civil forfeiture, securities...
- Counsel may be asked to receive, hold and transfer cryptocurrency (e.g., pending outcome of a dispute, as part of a settlement)
- Clients may wish to pay using cryptocurrency
- Goal today is to help you navigate questions involving cryptocurrency in your litigation practice, particularly AML considerations

Crypto 101

Blockchains and Cryptocurrencies

- Bitcoin was the first cryptocurrency
- Now there are hundreds (e.g. Ethereum, Litecoin, Bitcoin Cash, Ripple, Zcash, Dash, Monero)
- A blockchain is a type of database (or ledger).
- Blockchains exist on a decentralized network of nodes (computers).
- Every node keeps a copy of the blockchain, which records full history of transactions.



Blockchain Transactions

- Blockchain transactions are disintermediated and recorded on a decentralized ledger.
- Cryptocurrency and other blockchain transactions based on public key cryptography. To transfer cryptocurrency from Person A to Person B:
 - Person A creates a transaction to send coins to an address provided by Person B.
 - Person A signs the transaction with their private key.
 - Person A publishes the transaction to the network.
 - Person B waits for the transaction to be confirmed by the network.
- The private key provides control of the asset.

Crypto Wallets

- Wallets are software applications that simplify holding and transferring cryptocurrency by:
 - Tracking the private keys associated with addresses.
 - Calculating balances at addresses controlled by the wallet owner.
 - Generating new addresses and associated private keys.
 - Constructing and signing transactions using recipients' addresses.
 - Publishing transactions to the network.

Attributes of Blockchain Networks

- (Usually) Pseudonymous
 - Transactions on the blockchain use alphanumeric addresses, not names
- Immutable
 - A transaction cannot be reversed (except by the person who received the cryptocurrency)
- Decentralized
 - Consensus rules and mining/staking remove the need for a trusted third party

Crypto Exchanges / Trading Platforms

- Trading of cryptocurrencies has historically taken place primarily on centralized crypto exchanges / trading platforms
 - Combine custody, trade execution and settlement within a single platform
 - Trades generally not recorded on the blockchain
 - Platform has control of clients' assets
- Cryptocurrencies are also traded in other ways
 - “Over the counter” – Trades are settled by transferring crypto on the blockchain
 - “Decentralized Finance” – Trades are effected by “smart contracts” running on the blockchain
 - Peer to peer – Individuals can transfer crypto to each other without an intermediary

Anonymity – fact or fiction?

Anonymity of cryptocurrency transactions?

- Transactions on the blockchain are identified by alphanumeric addresses, not names.
- However, the transactions between addresses are generally transparent.
- So, if you can associate a real-world identity with a single transaction, you may be able to identify the owner of the address.

New tech, same problems...

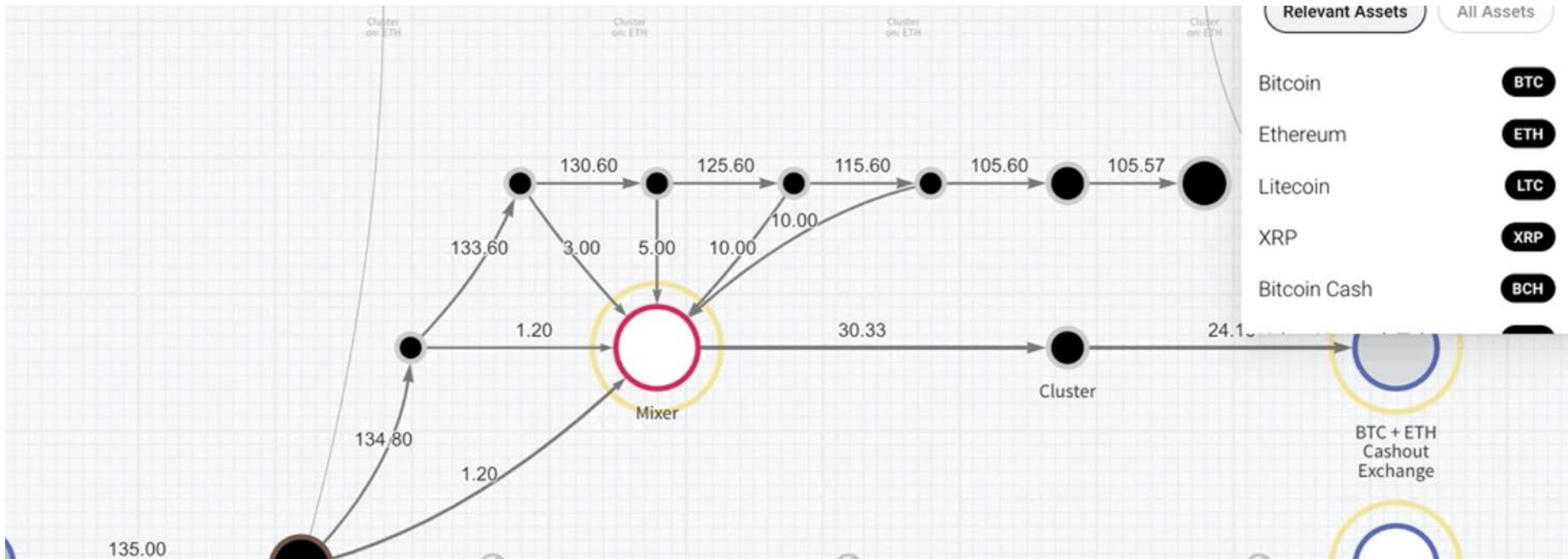
- Usually, transactions themselves are transparent once they get to the “crypto” stage and recorded on the blockchain
- But...
 - It is like a room full of people walking around conducting transactions while monitored by CCTV but they are all wearing disguises.
 - Or...Cryptocurrency is like a burner phone. We can observe device activity but it is difficult to know who is using it.

Blockchain Tracing / Blockchain Intelligence

- Various tools and techniques have been developed to “trace” and otherwise interpret blockchain transactions
 - Addresses “labelled” as associated with specific entities / activities
 - Different transactions / addresses can be grouped/clustered as relating to a single entity
- Blockchain intelligence tools are used by various entities:
 - By entities with AML/CTF/sanctions obligations for risk assessments
 - By law enforcement and national security organizations for investigative and intelligence-gathering purposes
 - By investigators for asset tracing and recovery
 - By commercial actors to derive business and market intelligence
 - By researchers seeking to understand economic and other activity on blockchains

Anonymity of cryptocurrency transactions?

Blockchain visualization tools can quickly and automatically display the relationships between addresses. This is an image from Chainalysis Reactor.



The potential problems

- The use of these tools raise a number of yet-to-be-answered legal problems. Some of these issues are now being litigated in other jurisdictions.
- For example:
 - Concerns over accuracy and the practical realities of “tracing”
 - Issues created by laundering techniques
 - “Proving” the trace in court
 - The authenticity and admissibility of blockchain evidence
 - The reliability and lawfulness of “attributions”
 - Does crypto tracing constitute a “search”?

Admissibility of Blockchain Tracing Evidence

- Is blockchain tracing evidence admissible as expert evidence?
 - Tracing techniques and heuristics are novel and developing
 - *R v Mohan* and *R v J.-L.J.*: “expert evidence which advances a novel scientific theory or technique is subjected to special scrutiny to determine whether it meets a basic threshold of reliability”
 - Tracing tools rely on databases of labelled address – are the labels hearsay?
- *R v Phan*, Ont. S.C.J., Court File CR-17-10000415 (April 3, 2019)
 - Phan pleaded guilty to firearms and drug offences
 - Forensic expert testified most of 288.64 BTC in Phan’s wallet traceable to dark markets
 - Court inferred BTC was proceeds of crime, which was forfeited to the Crown.
 - No responding expert evidence.
 - Decision did not discuss the reliability of the techniques used or admissibility of evidence that dark markets were associated with certain addresses.

Deanonymizing transactions: The production order route

Brecknell

- The RCMP wanted to obtain data from Craigslist, a U.S.-based company. Craigslist advised the police that they would comply with a Canadian production order for the data.
- The question presented was whether a Canadian court nevertheless had jurisdiction to grant the order, in the sense that a domestic production order could extend to a U.S.-based company and data located anywhere in the world.
- The B.C. Court of Appeal held that a domestic production order is enforceable against foreign entities so long as they have a real and substantial “virtual” connection to Canada and possession or control over the sought-after data (regardless of its location).

“Virtual Presence”

- In *Re TextPlus*, the Ontario Superior Court endorsed *Brecknell* and held that Canadian-based courts have jurisdiction under the *Criminal Code* to issue orders against foreign companies with only a real and substantial “virtual presence” in Canada.
- Binding on SCJ and OCJ judges and JPs in Ontario.

Two potential problems...

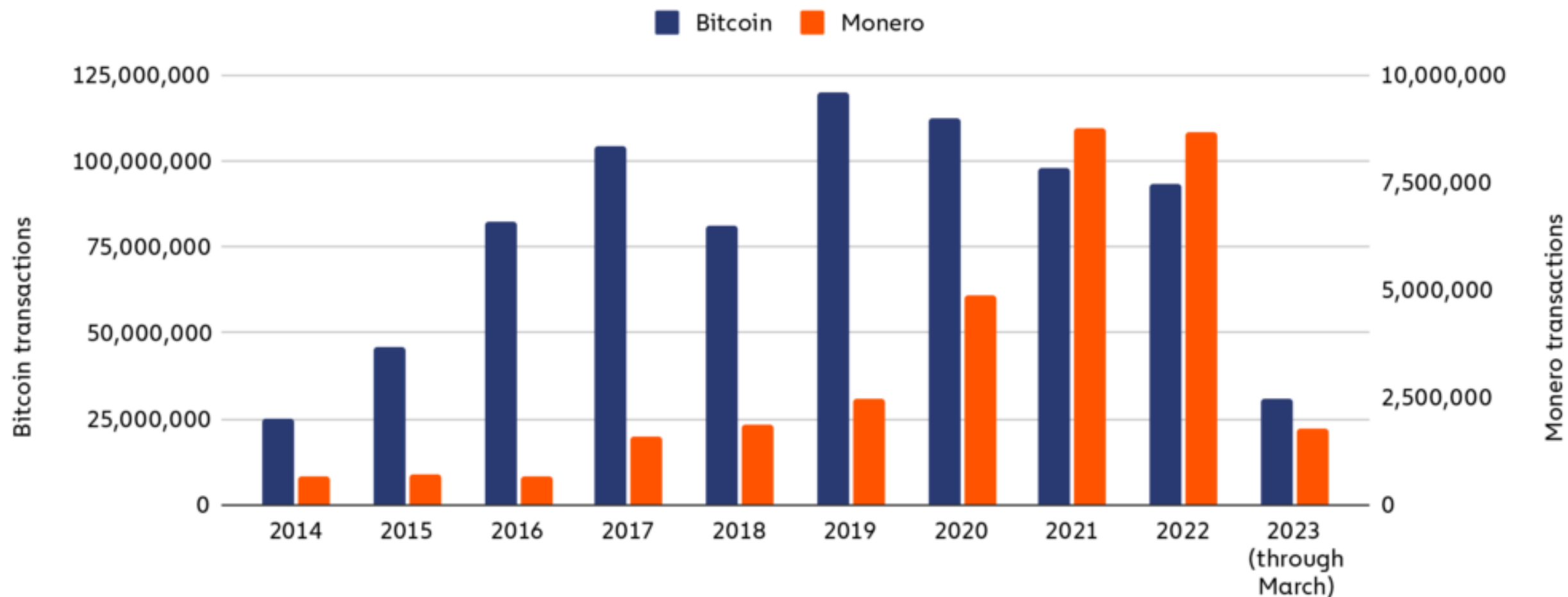
- First, line drawing. What counts as a real and substantial “virtual” presence.
- Second, enforcement. What to do when a foreign-based company simply refuses to acknowledge or comply with the court order? Discussion of past examples.
- . . . One solution: The *Cloud Act*?

AML/CTF & Other Risks

Financial Crime, Sanctions and National Security Considerations

- Cryptocurrencies can create potential financial crime, sanctions and national security risks because:
 - May allow layering and placement of proceeds of crime
 - May allow proceeds of fraud and other crimes to be removed beyond effective reach of law enforcement and courts
 - May allow transfers of value involving organized crime, terrorism or sanctioned entities
- Blockchains may also facilitate investigations and monitoring because blockchain transactions are permanent and public*
 - Some blockchains (ZCash, Monero) are designed to allow transactions without publicly revealing the source and recipient
 - Various means exist to complicate/prevent tracing (Tornado Cash, CoinJoin)
 - Off-chain transactions (e.g., trades on trading platforms) are not publicly available
 - Individual peer-to-peer transactions generally fall outside of AML regimes
 - Many trading platforms operate from foreign jurisdictions and may not cooperate

Transactions per year: Bitcoin vs. Monero, 2014 - 2023



© Chainalysis

Canadian Regulatory Regimes

- AML/CTF (*Proceeds of Crime (Money Laundering) and Terrorist Financing Act*)
 - Dealers in “virtual currency” required to register as money services businesses, implement compliance programs and report as required to FINTRAC
 - Applies to “foreign MSBs” that direct services to Canadians
- Securities
 - Some cryptocurrencies may be securities or derivatives under provincial securities laws
 - Crypto trading platforms that act as intermediaries for Canadian clients must register as securities dealers

What if my client wants to give me crypto?

- Law Society By-Law 7.1 – client identification and verification
 - Crypto assets are “funds”
 - Enhanced client ID, source of funds, and verification obligations kick in “when the licensee engages in or gives instructions in respect of the receiving, paying or transferring of funds”
 - Some exceptions (e.g. funds for legal fees)
 - Funds are exempt that are “paid to or received from a financial institution”
 - Funds are exempt that are “paid, received or transferred by electronic funds transfer”
 - Are crypto exchanges “financial institutions”?
 - When will a transfer of crypto be an “electronic funds transfer”?

Criminal Seizure and Forfeiture

The history

- Cryptocurrency seizures in the criminal context are new. See Colonial Pipeline.
- In Canada, the first crypto seizures happened in 2021.
- Two scenarios: (1) exchange seizures; (2) target seizures.
- Examples:
 - Durham Remote Desktop Takeover
 - Netwalker
 - Freedom Convoy

The General Warrant Approach

- Since 2021, GWs were used predominately to carry out crypto seizures. Over a dozen seizures.
- It appears a restraint order was used only once, early in 2021.

In re Binance

- Investigation into online fraud involving cryptocurrency romance and investment scam.
- Stolen funds in possession of Binance. Binance was prepared to comply with the orders. There was no dispute that the offences occurred and that the identified funds were in fact proceeds.
- Application judge denied general warrant and issued published decision holding that a general warrant cannot “stretch” to cover a cryptocurrency seizure. The judge questioned the police practice of using general warrants to seize digital proceeds.

The result

- As a general matter, cryptocurrency seizures are on hold in the province of Ontario. No seizure since March 2023 since no viable way to seize funds.
- The decision on appeal. Argued August 8, 2023.
- On reserve.

The new digital asset “search warrant”

- Came into force end of September 2023
- Designed to remedy this problem and create a specific tool for seizing cryptocurrency

Some questions...

- Crown applications v. police applications
- “In the province” requirement
- Forfeiture requirement
- AG undertakings

Clarity?

- This summer, the federal government conducted a consultation on a variety of cyber-related issues, including digital asset seizures.
- But with any legislative initiative, nothing is certain.
- Possible changes Fall 2023 and 2024?

Preservation & Civil Forfeiture

Cryptocurrency as Property – Proprietary Remedies

AA v Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019)

59. The conclusion that was expressed was that a crypto asset might not be a thing in action on a narrow definition of that term, but that does not mean that it cannot be treated as property. Essentially, and for the reasons identified in that legal statement, I consider that a crypto asset such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175 as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence. That too, was the conclusion of the Singapore International Commercial Court in *B2C2 Limited v Quoine PTC Limited* [2019] SGHC (I) 03 [142].

Preservation – *Mareva* Order

Li et al. v. Barber et. al., 2022 ONSC 1176

[23] Digital funds are not immune from execution and seizure to satisfy a debt any more than a bank account provided the individual or institution which can access the funds are within the reach of a court order. Digital wallets may be self controlled, but more commonly are part of a service provided by a provider and accessed through an application or software in a similar manner to online banking. Cryptocurrency exchanges are used to convert bitcoin or other currencies to fiat currency. Many of these digital institutions are within the jurisdiction of the court or are located in jurisdictions where Ontario judgments and orders may be enforced. The defendants of course are themselves subject to the jurisdiction of the court because they are present in Ontario and they may be enjoined from cashing or transferring assets including cryptocurrency.

Preservation – Compelled Disclosure / Transfer

- What if the crypto isn't held on a trading platform?

Autorités des marchés financiers et Lacroix, 2018 QCCS 3894 (CanLII)

- Judge appointed provisional administrator to take possession of certain property held by principal of PlexCoin
- Principal ordered to transfer 425 bitcoin to provisional administrator
- Principal failed to effect transfer; ultimately transfer occurred in a courtroom, under threat of contempt sanctions
- Can disclosure of private keys be compelled in the criminal context or does that infringe the right against self-incrimination?
 - Practically, private key material usually stored in an electronic device or a physical medium (paper, metal) – not memorized

Preservation – *Anton Piller* Order

Cicada 137 LLC v. Medjedovic, 2022 ONSC 369

[43] The plaintiff has already established the requisite elements required for an Anton Piller order including showing a strong prima facie case of unlawful conduct by the defendant. The court has ordered the defendant to turn over the disputed cryptocurrency tokens to be held by a neutral officer pending determination of whether the code is law or if he broke the law. The defendant has shown that he is not willing to comply with the court's order; that he will hide himself to avoid accountability; that he is not willing to stand up responsibly to establish the lawfulness of his conduct; and that he is willing to move the disputed tokens.



Law Society
of Ontario

Barreau
de l'Ontario

TAB 2

Anti-Money Laundering: Protecting Your Litigation Practice

**FINTRAC Disclosures: Results through Financial
Intelligence (PowerPoint)**

Michael Boole, Manager – Anti-Money Laundering Unit
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

October 17, 2023





Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada

FINTRAC DISCLOSURES: Results through Financial Intelligence

2,292

unique financial intelligence
disclosures in 2021–22



Financial intelligence
disclosures often contain
**hundreds or even
thousands** of financial
transaction reports in
each package



to municipal, provincial and federal
law enforcement in British Columbia
in 2021–22:

- » **890 individuals**, more than
30,000 transaction reports
- » approximate value in the
transactions: **\$2.88 billion**



major investigations
throughout Canada in
2021–22 and many hundreds
of individual investigations
across the country

Provided more than
24,000

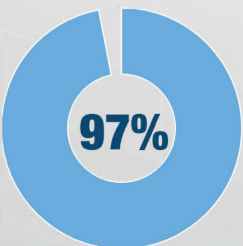
financial intelligence disclosures
to Canada's law enforcement and
national security agencies **since 2001**



Received

2,168

**voluntary information
records** from Canada's
law enforcement and
national security agencies



of the feedback that
FINTRAC received last year
from disclosure recipients
indicated that its financial
intelligence was both
valuable and actionable

PUBLIC-PRIVATE PARTNERSHIPS

Produced

757

financial intelligence disclosures
related to Canada's public-private
partnerships created to combat:



- ❖ Human Trafficking for Sexual Exploitation
- ❖ Romance Fraud
- ❖ Trafficking of Illicit Fentanyl
- ❖ ML in BC and Across Canada (Underground banking)
- ❖ Online Child Sexual Exploitation
- ❖ Illicit Cannabis
- ❖ Wildlife Trafficking

PROJECT SOUTHAM



The OPP recognized FINTRAC's contribution
to Project Southam:

- » Where organized crime groups allegedly
**imported high volumes of
cocaine and committed other
criminal activities**
- » **22 people** charged with

139 offences

Canada

Key Budget 2023 Highlights:

- ❖ New criminal offence for structuring financial transactions to avoid reporting to FINTRAC;
- ❖ Strengthening the registration framework for currency dealers and other MSBs to prevent their abuse;
- ❖ Criminalizing the operation of unregistered MSBs;
- ❖ Establishing authorities for FINTRAC to disseminate strategic analysis related to the financing of threats to the safety of Canada;
- ❖ Providing whistleblowing protections for employees who report information to FINTRAC;
- ❖ Broadening the use of FINTRAC non compliance disclosures in criminal investigations;
- ❖ Setting up obligations for the financial sector to report sanctions related information to FINTRAC
- ❖ Improving the sharing of compliance information between FINTRAC, OSFI and the Minister of Finance;
- ❖ Designating OSFI as a recipient of FINTRAC disclosures pertaining to threats to the security of Canada, where relevant to OSFI's responsibilities;



Law Society
of Ontario

Barreau
de l'Ontario

TAB 3

Anti-Money Laundering: Protecting Your Litigation Practice

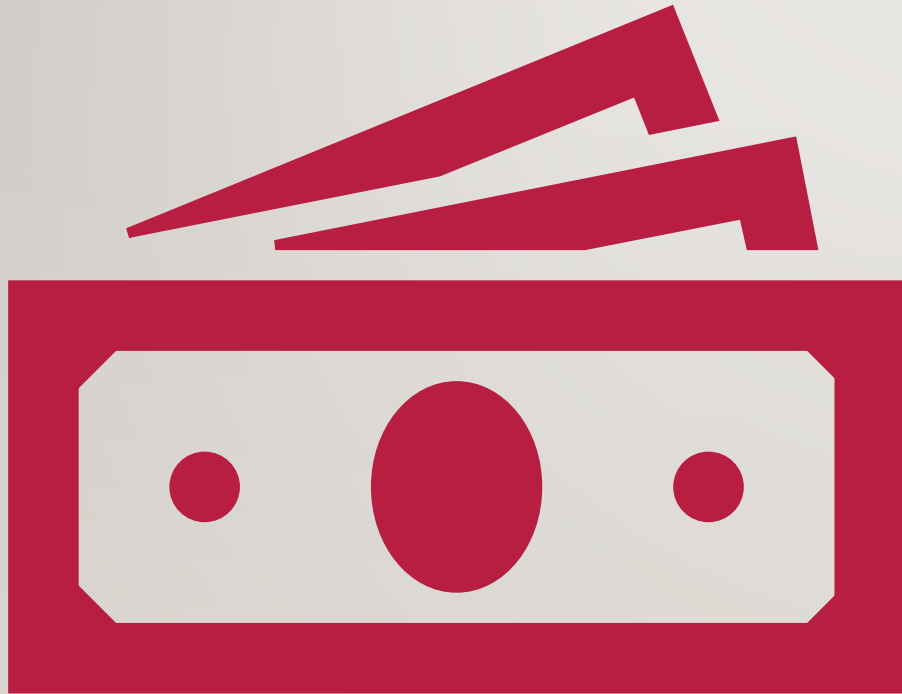
Money Laundering
Criminal Prosecutions (PowerPoint)

Benjamin Lerer, Crown Counsel, Serious Fraud Office
Ministry of the Attorney General

Lynda Morgan
Addario Law Group LLP

October 17, 2023





MONEY LAUNDERING

CRIMINAL PROSECUTIONS

AGENDA

1. The Criminal Offence

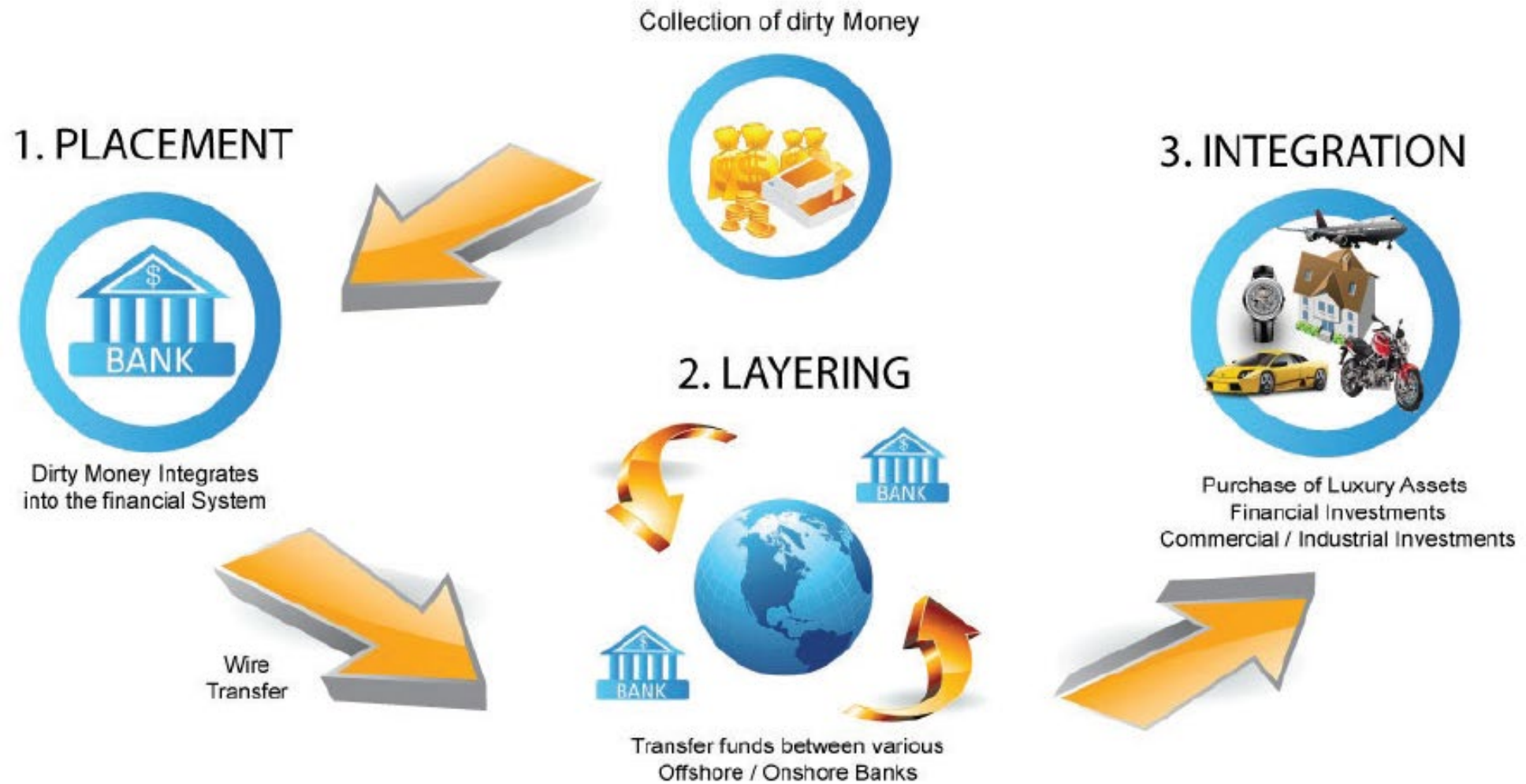
2. Recent Trends

3. Practical Issues

PART I

DEFINING THE CRIMINAL OFFENCE

A TYPICAL MONEY LAUNDERING SCHEME



A TYPICAL MONEY LAUNDERING SCHEME

Collection of dirty Money



1. PLACEMENT



Dirty Money Integrates into the financial System

Wire Transfer

2. LAYERING



Transfer funds between various Offshore / Onshore Banks

3. INTEGRATION



Purchase of Luxury Assets
Financial Investments
Commercial / Industrial Investments

“LAUNDERING PROCEEDS OF CRIME” (462.31)

- Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of
 - **(a)** the commission in Canada of a designated offence;
 - **(b)** an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.



I. DEALING WITH PROPERTY OR PROCEEDS

- Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of
 - (a) the commission in Canada of a designated offence;
 - (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.



I. DEALING WITH PROPERTY OR PROCEEDS

Property = Anything of Value

Deal With = Almost Any Act.



2. INTENT TO CONVERT OR CONCEAL

- Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property **with intent to conceal or convert that property or those proceeds**, knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of
 - **(a)** the commission in Canada of a designated offence;
 - **(b)** an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.



2. INTENT TO CONVERT OR CONCEAL

- Conversion = Change Form
- Concealment = Hide the Source



3. KNOWLEDGE, BELIEF AND RECKLESSNESS

- Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, **knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of**
 - **(a) the commission in Canada of a designated offence;**
 - **(b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.**



3. KNOWLEDGE, BELIEF AND RECKLESSNESS

- Designated Offence = Any Indictable Offence
- Can trace property as it changes form.
(e.g. Lottery Ticket → Jackpot)



3. KNOWLEDGE, BELIEF AND RECKLESSNESS

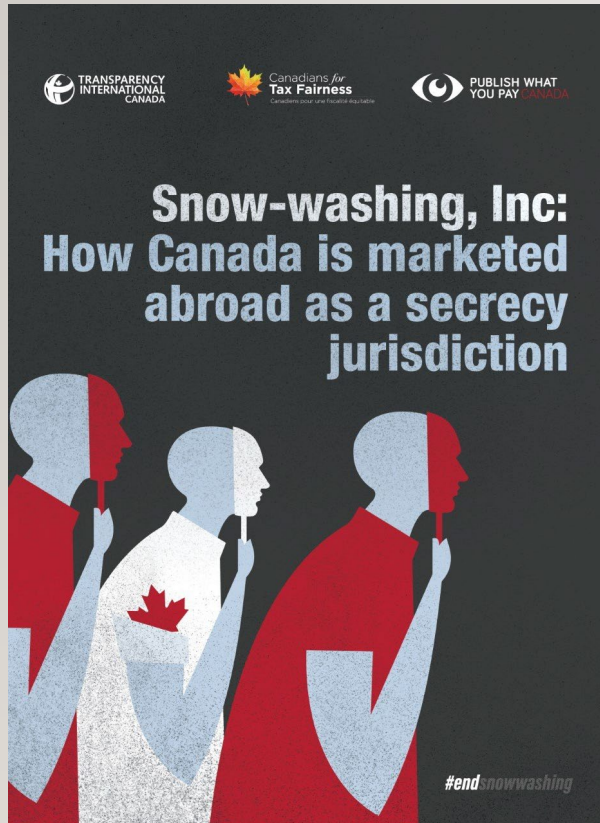
Mens Rea	Definition
Knowledge	Obtained by crime, and you knew it
Recklessness	Obtained by crime, and you knew there was a risk
Belief	You believed it was obtained by crime, regardless of the actual origin
Willful Blindness	You were suspicious about the property, but deliberately chose to remain ignorant.



PART II

RECENT TRENDS

MONEY LAUNDERING IN BRITISH COLUMBIA



Snow Washing

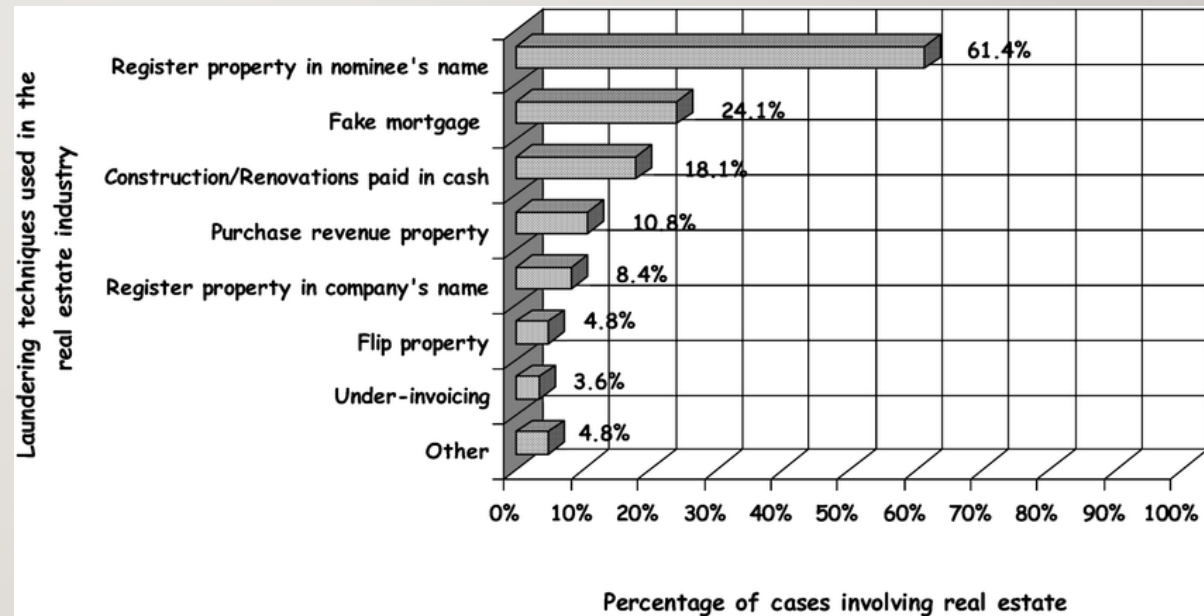
The Vancouver Model – Casinos

The Vancouver Model – Renovations

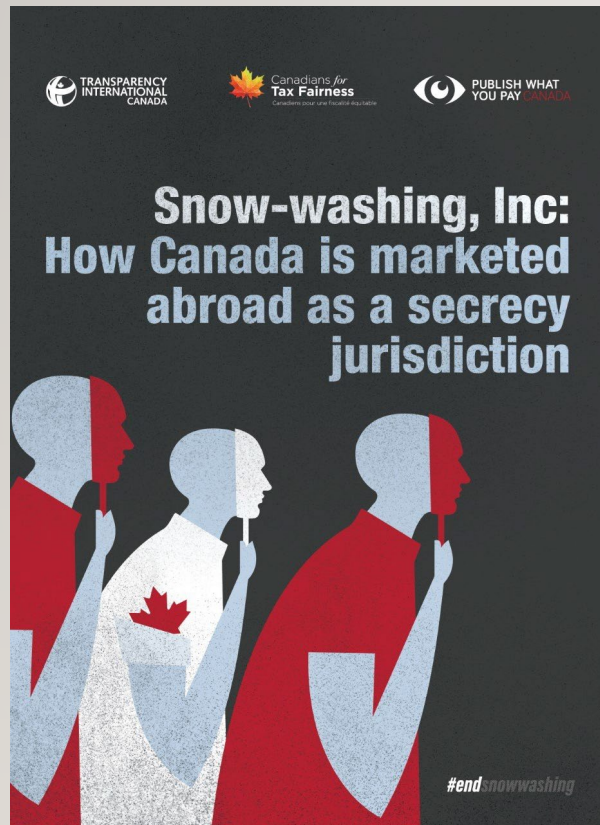
Luxury Vehicles and Horse Racing

CANADIAN ML TRENDS

- Structured Transactions
- Smurfs
- Undervalued Assets
- Nominee Property Owners
- Nominee Corporate Administrators
- False Mortgages / Liens



LEGISLATIVE DEVELOPMENTS



BC Beneficial Ownership Registry

US Corporate Transparency Act

Federal Registry of Beneficial Ownership (2025)

Unexplained Wealth Orders (BC)

PART III

Practical Issues

RECEIVING CLIENT FUNDS

PCMLTFA Overturned

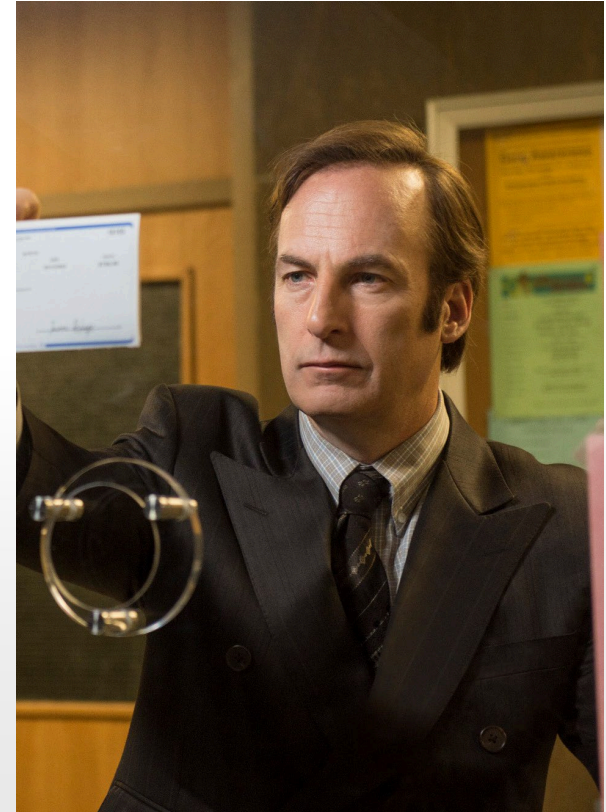
- *Canada v FLSC*, 2015 SCC 7
- Lawyers exempt from retaining, reporting, and searches

LSO Bylaw 7.1

- Nature of Business
- Direct and Indirect Ownership
- Source of funds being Received, Paid, or Transferred

Wilful Blindness

- *Ste Marie c. R.*, 2022 QCCA 1137
- If you *don't* ask about the source of funds, you might be laundering.



PRE-CHARGE ISSUES

Remediation Agreements

Compelled Evidence

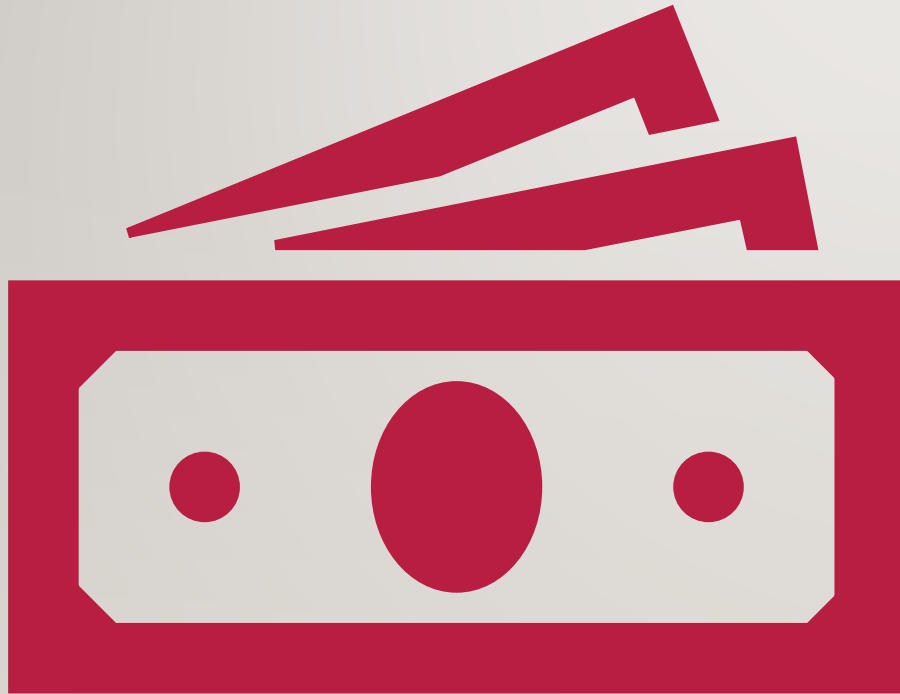
Responding to Warrants

POST-CHARGE ISSUES

Wagg Applications

Ancillary Orders

Civil Forfeiture



Ben Lerer – Crown Counsel,
Serious Fraud Office

benjamin.lerer@ontario.ca

Lynda Morgan – Partner, Addario
Law Group

lmorgan@addario.ca



Law Society
of Ontario

Barreau
de l'Ontario

TAB 4

Anti-Money Laundering: Protecting Your Litigation Practice

Weblinks to Department of Finance Consultation Papers
and Stakeholder Submissions on Strengthening
Canada's Anti-Money Laundering and
Anti-Terrorist Financing Regime

Paul Saguil, AVP
TD Bank Group

October 17, 2023



Weblinks to Department of Finance Consultation Papers and Stakeholder Submissions on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Submitted by: Paul Saguil, AVP, *TD Bank Group*

1. Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime - Process (Government of Canada)

<https://www.canada.ca/en/department-finance/programs/consultations/2023/strengthening-canada-anti-money-laundering-and-anti-terrorist-financing-regime/consultation-on-strengthening-canadas-anti-money-laundering-anti-terrorist-financing-regime.html>

2. Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime – Key questions for consideration (Government of Canada)

<https://www.canada.ca/en/department-finance/programs/consultations/2023/strengthening-canada-anti-money-laundering-and-anti-terrorist-financing-regime.html>

3. Improving Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, *The Canadian Bar Association*, August 2023

[https://www.cba.org/Our-Work/Submissions-\(1\)/Submissions/2023/August/Improving-Canada-s-Anti-Money-Laundering-and-Anti](https://www.cba.org/Our-Work/Submissions-(1)/Submissions/2023/August/Improving-Canada-s-Anti-Money-Laundering-and-Anti)

4. Limit Access to the Beneficial Ownership Registry, *The Canadian Bar Association*, September 26, 2023

<https://www.cba.org/Our-Work/cbainfluence/Submissions/2023/September/Limit-access-to-the-beneficial-ownership-registry>

5. A Strong Banking System for a Strong Canada – A Pre-Budget Submission by the Canadian Bankers Association, *Canadian Bankers Association*, August 4, 2023

[A Strong Banking System for a Strong Canada - A Pre-Budget Submission by the Canadian Bankers Association | A Strong Banking System for a Strong Canada - A Pre-Budget Submission by the Canadian Bankers Association \(cba.ca\)](#)

6. Banks' efforts to prevent money laundering and terrorist financing, *Canadian Bankers Association*, July 29, 2019

[Banks' efforts to prevent money laundering and terrorist financing | Banks' efforts to prevent money laundering and terrorist financing \(cba.ca\)](#)



Law Society
of Ontario

Barreau
de l'Ontario

TAB 5

Anti-Money Laundering: Protecting Your Litigation Practice

Asset Forfeiture/Freezing

Melissa Adams, Crown Law Office – Criminal
Ministry of the Attorney General

Graeme Hamilton
Borden Ladner Gervais LLP

October 17, 2023



Asset Forfeiture/Freezing

Melissa Adams, Crown Law Office – Criminal, Ministry of the Attorney General
Graeme Hamilton, Borden Ladner Gervais LLP

CRIMINAL CODE, R.S.C., 1985, c. C-46

Pre-Trial Preservation of Proceeds of Crime¹

Restraint Order, section 462.33

- On application by the Attorney General, the court may issue a restraint order where satisfied that there are reasonable grounds to believe that there exists in or outside of Canada any property in respect of which an order of forfeiture under sections 462.37(1), (2.01) or 462.38(2) may be made in respect of a designated offence² alleged to have been committed in the province in which the restraint order is made.
- The restraint order prohibits any person from disposing of, or otherwise dealing with any interest in the property otherwise than in the manner specified in the order.
- Usually relates to intangible property.

Special Search Warrant, section 462.32

- On application by the Attorney General, the court may issue a special search warrant where satisfied that there are reasonable grounds to believe that there is in any building, receptacle or place, any property in respect of which an order of forfeiture may be made under sections 462.37(1), (2.01) or 462.38(2) in respect of a designated offence alleged to have been committed in the province in which the warrant is issued.
- The special search warrant may be executed in any province.
- Relates to tangible property.

Special Search Warrant (Digital Assets), section 462.321

- On application by the Attorney General, the court may issue a special search warrant where satisfied that there are reasonable grounds to believe that any digital assets, including virtual currency, may be the subject of a forfeiture order under sections 462.37(1), (2.01) or 462.38(2) in respect of a designated offence alleged to have been committed in the province in which the warrant is issued.
- The special search warrant authorizes the search by using a computer program, and the seizure by taking control of the right to access the digital assets.

¹ “**Proceeds of Crime**” is defined in section 462.3(1) of the *Criminal Code* as any property, benefit or advantage, within or outside Canada, obtained or derived directly or indirectly by the commission of a designated offence or an act or omission anywhere that would have been a designated offence if it had occurred in Canada.

² “**Designated Offence**” is defined in section 462.3(1) of the *Criminal Code* as any offence that may be prosecuted as an indictable offence under any Act of Parliament, other than indictable offences prescribed by regulation, or a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an indictable offence.

Forfeiture of Proceeds of Crime

Forfeiture Order, section 462.37(1)

- On application by the Attorney General and where there is a finding of guilt, the court shall order forfeiture if satisfied on a balance of probabilities that the property is proceeds of crime; and the designated offence was committed in relation to the property.

Forfeiture Order (Reverse Onus), section 462.37(2.01)

- On application by the Attorney General and where there is a finding of guilt for an enumerated offence (drug offences, criminal organization offences, human trafficking offences), the court shall order forfeiture of any property of the offender identified by the Attorney General if the court is satisfied on a balance of probabilities that:
 - Within 10 years prior to the proceedings in respect of which the offender is sentenced, the offender engaged in a pattern of criminal activity for the purpose of directly or indirectly receiving a material benefit; or
 - The income of the offender from sources unrelated to designated offences cannot reasonably account for the value of all the property of the offender.
- The court shall not make an order of forfeiture in respect of any property that the offender establishes, on a balance of probabilities, is not proceeds of crime.

Fine in Lieu of Forfeiture, section 462.37(3)

- Where there is a finding of guilt and where the court is satisfied that an order of forfeiture under section 462.37(1) or (2.01) should be made, but the property or part of the property cannot be made subject to a forfeiture order, the court may order the offender to pay a fine in any amount equal to the value of the property.

Forfeiture Order (In Rem), section 462.38(2)

- On application by the Attorney General, where an information is laid in respect of a designated offence, the court shall order forfeiture if satisfied, beyond a reasonable doubt, that the property is proceeds of crime in respect of the designated offence, and the accused charged with the designated offence has died or absconded.

Victim Compensation

Restitution Order, section 738

- On application by the Attorney General, where there is a finding of guilt, the court may order that the offender make restitution to another person.
- The court is required to consider restitution and shall inquire of the prosecutor if reasonable steps have been taken to provide the victims with an opportunity to indicate whether they are seeking restitution for their losses and damages, the amount of which must be readily ascertainable: section 737.1.

Priority to Restitution, section 462.49(2)

- The property of an offender may be used to satisfy a forfeiture order only to the extent that it is not required to satisfy the operation of any other provision of any Act of Parliament respecting the restitution to or compensation of persons affected by the commission of offences.

Preservation of Proceeds of Unlawful Activity³

Preservation Order, section 4

- In a motion by the Attorney General, within a proceeding commenced by the Attorney General, the court may make an interlocutory order for the preservation, management or disposition of any property that is the subject of the proceeding, including a restraint order, an order for possession, delivery or safekeeping of the property, an order appointing a receiver or manager for the property, etc.

Forfeiture of Proceeds of Unlawful Activity

Forfeiture Order, section 3

- In a proceeding commenced by the Attorney General, the court shall make an order forfeiting property that is in Ontario to the Crown in right of Ontario if the court finds that the property is proceeds of unlawful activity.

Administrative Forfeiture, sections 1.1 – 1.10

- The Attorney General may commence an administrative forfeiture proceeding where there is reason to believe that property located in Ontario is proceeds of unlawful activity.
- An administrative forfeiture proceeding is commenced by filing a notice on the *PPSA*, giving notice to the public, the person from whom the property was seized, the public body holding the property, and any other person who may have an interest in the property.
- If no notice of dispute is received by the imposed deadline, the property is forfeited to the Crown in right of Ontario.
- If a notice of dispute is received, the Attorney General shall either commence proceedings against the property or withdraw from seeking forfeiture of the property.

Victim Compensation

Compensation to Direct Victims of Unlawful Activity

- One of the purposes of the *Civil Remedies Act* is to provide civil remedies that will assist in compensating persons who suffer pecuniary or non-pecuniary losses as a result of unlawful activities.
- Where forfeiture ordered, a Statutory Notice is posted for victims to make a claim for compensation. Claims are adjudicated by an independent adjudicator appointed by regulation, who may approve, partially approve, or deny claims. Approved claims are distributed *pro-rata*.

³ “Instrument of Unlawful Activity” is defined in section 7 of the *Civil Remedies Act* as property that is likely to be used to engage in unlawful activity that, in turn, would be likely to or is intended to result in the acquisition of other property, in injury to the public or in serious bodily harm to any person, and includes any property that is realized from the sale or other disposition of such property.

Pre-Trial Preservation of Property in Civil Proceedings

Rules of Civil Procedure, r. 44

- An interim order for recovery of possession of personal property may be obtained on motion by the plaintiff, supported by an affidavit setting out: (a) a description of the property sufficient to make it readily identifiable, (b) the value of the property, (c) that the plaintiff is the owner or lawfully entitled to possession of the property, (d) that the property was unlawfully taken from the possession of the plaintiff or is unlawfully detained by the defendant, and (e) the facts and circumstances giving rise to the unlawful taking or detention.
- A codification of the former common law action for replevin.

Rules of Civil Procedure, r. 45

- Under r. 45.01(1), the Court may make an interim order for the custody or preservation of any property in question in a proceeding or relevant to an issue in a proceeding, and for that purpose may authorize entry on or into any property in the possession of a party or of a person not a party.
- Under r. 45.02, where the right of a party to a specific fund (i.e. an identifiable fund or pool or money that is at issue in litigation, such as a bank account, funds in a trust account, a deposit) is in question, the Court may order the fund to be paid into Court or otherwise secured on such terms as are just.

Anton Piller Order

- A type of injunction that allows the moving party to search for and seize property in order to preserve that party's rights in property pending the determination of the proceeding.
- Allows party to enter premises of opposing party to seize property.
- Higher threshold than an order under r. 45.01: requires strong *prima facie* case.

Mareva Injunction

- A type of injunction that freezes the defendant's assets or a portion thereof prior to trial.
- Higher threshold than an order under r. 45.02: requires *strong prima facie* case. Also requires showing that there are existent assets and that there is a risk that they will be dissipated prior to trial.



Law Society
of Ontario

Barreau
de l'Ontario

TAB 6

Anti-Money Laundering: Protecting Your Litigation Practice

Law Society AML Resources

8 Tips to Help Verify the Identity of an Individual

Phil Brown, Acting Director, Practice Supports & Resources
Law Society of Ontario

October 17, 2023



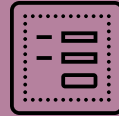
Law Society AML Resources

The below Law Society resources can help you understand and comply with your client identification and verification obligations.



Flowchart

Overview of the steps required to comply with ID/Verify Requirements



File Forms

File Forms to record steps taken to comply with ID/Verify, source of funds and monitoring obligations



Glossary

Definitions for common AML terms



Precedent

Sample agreement for using an agent to help identify or verify the identity of an individual



Examples

Examples of appropriate government-issued photo ID and reliable sources of information



Worksheet

Worksheet to help spot red flags of fraud and other illegal conduct and record due diligence efforts



FAQs

Over 100 Frequently Asked Questions on ID/Verify, source of funds, and monitoring



Case Studies

Case studies to learn how to identify red flags and what steps to take when faced with a possible fraud



8 Tips to Help Verify the Identity of an Individual



#1.

Does the client have an Ontario driver's license? If so, confirm its status [here](#).



#5.

Compare the photo on the ID to the client and check for noticeable differences (e.g. facial features)



#2.

Check if the person has a neutral expression in their photo ID as this is usually a requirement



#6.

Check for inconsistencies in the numbers and letters (weight, font, and colour) on the ID



#3.

Look for differences in the how the client's name is spelled on the ID



#7.

Visit the [AGCO's website](#) for tips on checking photo ID in-person



#4.

Check the signature on the ID and see if it is similar to your clients



#8.

If verifying identity virtually or viewing ID from a different country consider utilizing [authentication technology](#) to help detect fraud

