

**PROCEEDINGS AT HEARING  
OF  
NOVEMBER 23, 2020**

**COMMISSIONER AUSTIN F. CULLEN**

**INDEX OF PROCEEDINGS**

| <b>Witness</b>   | <b>Description</b>                                      | <b>Page</b> |
|--|---|-------------|
|  | Proceedings commenced at 9:30 a.m.                      | 1           |
|  | Discussion re exhibits                                  | 1           |
|  | Discussion re witnesses                                 | 3           |
|  | Discussion re procedure                                 | 4           |
| <b>Aaron Gilkes<br/>(for the commission)<br/>Adrienne Vickery<br/>(for the commission)<br/>Warren Krahenbil<br/>(for the commission)</b> | Examination by Mr. Martland                             | 5           |
|  | Proceedings adjourned at 11:17 a.m.                     | 85          |
|  | Proceedings reconvened at 11:26 a.m.                    | 85          |
| <b>Aaron Gilkes<br/>(for the commission)<br/>Adrienne Vickery<br/>(for the commission)<br/>Warren Krahenbil<br/>(for the commission)</b> | Examination by Mr. Martland (continuing)                | 86          |
|  | Examination by Ms. Harlington                           | 152         |
|  | Examination by Ms. Magonet                              | 159         |
|  | Examination by Mr. Gratl                                | 172         |
|  | Discussion re examinations                              | 193         |
|  | Proceedings adjourned at 1:49 p.m. to November 24, 2020 | 194         |

## INDEX OF EXHIBITS FOR IDENTIFICATION

| Letter | Description | Page |
|--------|-------------|------|
|--------|-------------|------|

No exhibits for identification marked.

## INDEX OF EXHIBITS

| No. | Description   | Page |
|-----|---|------|
| 246 | Overview Report - Quadriga CX   | 2    |
| 247 | Overview Report - Canadian Securities Administrators Publications on Virtual Assets | 2    |
| 248 | Overview Report - FATF Publications on Virtual Assets                               | 2    |
| 249 | Overview Report - Federal Regulation of Virtual Currencies                          | 3    |
| 250 | Curriculum Vitae of Sgt. Adrienne Vickery   | 7    |
| 251 | Curriculum Vitae of Cpl. Aaron Gilkes   | 10   |
| 252 | Curriculum Vitae of Cpl. Aaron Gilkes   | 11   |
| 253 | RCMP Virtual Assets Slideshow   | 13   |
| 254 | Senate Report - Digital Currency You Can't Flip this Coin! - June 2015              | 171  |

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

**November 23, 2020**

**(Via Videoconference)**

**(PROCEEDINGS COMMENCED AT 9:30 A.M.)**

THE REGISTRAR: The hearing is now resumed.  
Mr. Commissioner.

THE COMMISSIONER: Thank you, Madam Registrar.

Yes, Mr. Martland, I see you are joined by  
Ms. Rose and Ms. Patel.

MR. MARTLAND: Yes. Thank you, Mr. Commissioner.

And we are embarking on hearings now that turn  
the focus of our process to virtual assets,  
sometimes also referred to as cryptocurrency.  
And we begin that topic -- first I'll speak to  
one or two procedural things, and then we can  
commence with the evidence of the panel of three  
witnesses today.

First, by way of speaking to overview  
reports on this topic area, pursuant to Rule 33,  
overview reports have been circulated to  
participants in draft format and we've  
benefitted from input from participants on those  
reports. We are now in a position to ask that  
those please be marked as exhibits. Madam  
Registrar has facilitated this with a list of  
the three overview reports, which you'll

1                   probably see on the screenshare right now.

2                   First is -- proposed as the next exhibit,

3                   overview report with respect to Quadriga CX.

4           THE COMMISSIONER: Very well. That will be

5                   exhibit 246.

6           THE REGISTRAR: Exhibit 246.

7                   **EXHIBIT 246: Overview Report - Quadriga CX**

8           MR. MARTLAND: Secondly, the overview report, virtual

9                   assets regarding the Canadian Securities

10                  Administrators guidance.

11           THE COMMISSIONER: 247.

12           THE REGISTRAR: Exhibit 247.

13                   **EXHIBIT 247: Overview Report - Canadian**

14                   **Securities Administrators Publications on**

15                   **Virtual Assets**

16           MR. MARTLAND: Thank you. Third, the overview report

17                   on virtual assets regarding the FATF and DOJ

18                   documents.

19           THE COMMISSIONER: 248.

20           THE REGISTRAR: Exhibit 248.

21                   **EXHIBIT 248: Overview Report - FATF**

22                   **Publications on Virtual Assets**

23           MR. MARTLAND: And finally the overview report on

24                   Federal regulation of virtual currencies.

25           THE COMMISSIONER: 249.

1 THE REGISTRAR: Exhibit 249.

2 **EXHIBIT 249: Overview Report - Federal**

3 **Regulation of Virtual Currencies**

4 MR. MARTLAND: Thank you. We can now move into  
5 today's hearing with three member of the RCMP:  
6 Sergeant Adrienne Vickery, Sergeant Warren  
7 Krahenbil -- and I should pause to ask Officer  
8 Krahenbil how badly I'm mispronouncing his name,  
9 perhaps. That might be something to address at  
10 the outset.

11 THE WITNESS: (WK) That was just fine.

12 MR. MARTLAND: Was it? All right. That's nice of  
13 you to say. And Acting Sergeant Aaron Gilkes is  
14 joining us as well.

15 And, Madam Registrar, all three witnesses  
16 have asked to be affirmed, please.

17 THE REGISTRAR: Would each of you please state your  
18 full name and spell your first name and last  
19 name for the record. I'll start with Corporal  
20 Gilkes.

21 THE WITNESS: (AG) Aaron Gilkes. First name Aaron,  
22 A-a-r-o-n. Last name Gilkes, G-i-l-k-e-s.

23 THE REGISTRAR: Thank you. And Sergeant Vickery.

24 THE WITNESS: (AV) good day. Adrienne Vickery.  
25 A-d-r-i-e-n-n-e. Last name V-i-c-k-e-r-y.

Aaron Gilkes (for the commission)  
Adrienne Vickery (for the commission)  
Warren Krahenbil (for the commission)  
Discussion re procedure

1 THE REGISTRAR: Thank you. And Sergeant Krahenbil.

2 THE WITNESS: (WK) Warren Krahenbil, W-a-r-r-e-n

3 K-r-a-h-e-n-b-i-l.

4 THE REGISTRAR: Thank you.

5 AARON GILKES, a witness  
6 called for the  
7 commission, affirmed.

8 ADRIENNE VICKERY, a  
9 witness called for the  
10 commission, affirmed.

11 WARREN KRAHENBIL, a  
12 witness called for the  
13 commission, affirmed.

14 MR. MARTLAND: Thank you. Mr. Commissioner, with  
15 respect to the evidence this week unlike some of  
16 the prior hearings, we've organized things in a  
17 way that the documents for today's panel, at  
18 least, does not contain documents where we need  
19 to be cautious about having them shared with --  
20 more broadly on to the webcast of these  
21 hearings. And so my expectation as we go  
22 forward is that the documents I'm putting  
23 forward can be displayed both on the Zoom  
24 screenshare with participants that are on that  
25 platform but also through the webcast out. And

Aaron Gilkes (for the commission)  
Adrienne Vickery (for the commission)  
Warren Krahenbil (for the commission)  
Discussion re procedure  
Exam by Mr. Martland

5

1                   as we mark exhibits, likewise I don't see any  
2                   expectation that we would need to have a delay  
3                   to permit a redactions process. To the extent  
4                   there were a few redactions to address, or at  
5                   least contact information, those have already  
6                   been made to the proposed exhibits.

7                   THE COMMISSIONER: All right. Thank you.

8                   MR. MARTLAND: I'll begin with -- to give a bit of a  
9                   lay of the land for today. I'm enormously  
10                  assisted by the fact that the witnesses have  
11                  prepared a PowerPoint presentation, which will  
12                  be a very useful way to walk through topics in  
13                  evidence today. So what I propose to do is  
14                  first to spend a little time with a biographical  
15                  sketch of each of the three witnesses, including  
16                  marking their CVs, and then turn to that  
17                  PowerPoint and use that as the means to lead the  
18                  evidence through the panel.

19                  THE COMMISSIONER: All right. Thank you.

20                  **EXAMINATION BY MR. MARTLAND:**

21                  Q     So first I'll start with Sergeant Vickery,  
22                  please. Sergeant, you are the RCMP National  
23                  Cryptocurrency Coordinator assigned to national  
24                  headquarters in Ottawa, Federal Policing  
25                  Criminal Operations and within the Financial

1 Crime, Proceeds of Crime/Money Laundering

2 Section. Is that accurate?

3 A (AV) Yes, that's correct.

4 Q You've served with the RCMP since 2005 in a

5 number of different positions, including

6 Commercial Crime, Serious and Organized Crime

7 Section, Financial Crime Section and the

8 National Security High-Risk Traveller Unit?

9 A (AV) That is correct.

10 Q And last five years you've served as the

11 national RCMP Money Laundering/Proceeds of Crime

12 Coordinator at national headquarters and in that

13 capacity providing program governance, training

14 development and policy development; is that

15 right?

16 A (AV) Yes.

17 Q Your role includes file review, operational

18 feedback of priority money laundering and

19 cryptocurrency files, and that's a role that

20 really spans the whole country?

21 A (AV) Yes, that is correct.

22 Q You also participate in the FATF, the Financial

23 Action Task Force, Europol, and with other

24 international law enforcement, and indeed you

25 lead the RCMP domestic working group on



1                   cryptocurrency based out of national  
2                   headquarters and serve as a member of the Five  
3                   Eyes Cryptocurrency Operational Readiness  
4                   Initiative?

5           A       (AV) Yes.

6           MR. MARTLAND:   And I'll ask Madam Registrar to please  
7                   have displayed on the screen your CV.

8           Q       (AV) And if I might simply confirm, Sergeant,  
9                   you recognize that as being your CV?

10          A       (AV) Yes, I do.

11          MR. MARTLAND:   I'll asking, Mr. Commissioner, that  
12                   please be marked as the next exhibit.

13          THE COMMISSIONER:   250.

14          THE REGISTRAR:   Exhibit 250.

15                   **EXHIBIT 250:   Curriculum Vitae of Sgt. Adrienne**  
16                   **Vickery**

17          MR. MARTLAND:

18          Q       Next, Acting Sergeant Gilkes, I'd ask that we --  
19                   I'll review a biographical sketch and then also  
20                   turn up your CV.   Your -- first with respect to  
21                   your rank, you're an acting sergeant and equally  
22                   corporal.   So I'll probably try and stick to one  
23                   or the other through this, but you hold both  
24                   ranks; is that correct?

25          A       (AG) Yes.   I am a corporal and acting sergeant

1 at the moment.

2 Q Thank you. You serve as a cybercrime instructor  
3 with the Canadian Police College in Ottawa and  
4 previously were a digital forensic supervisor  
5 with the "E" Division, which is the  
6 British Columbia arm of the RCMP; correct?

7 A (AG) That's correct.

8 Q And you've been with the RCMP since 2011, having  
9 served in roles both in "E" Division here in BC,  
10 "C" division in Quebec with their Proceeds of  
11 Crime unit and with the Integrated Technological  
12 Crime Unit?

13 A (AG) That is correct.

14 Q And by way of background, you had experience in  
15 the financial sector before joining the RCMP?

16 A (AG) That is correct.

17 Q Your role now, you supervise technological crime  
18 investigators, you're involved in development  
19 and training with respect to digital evidence  
20 acquisition methodologies and techniques and you  
21 also are involved in forensic examinations of  
22 digital devices and providing technological and  
23 computer forensic support for municipal law  
24 enforcement as well as "E" Division  
25 investigations?

1           A       (AG) That was my role when I was in "E"  
2                    Division.

3           Q       Okay. And so presently your role has shifted to  
4                    being focused on the police college in Ottawa?

5           A       (AG) That is correct. My current role is as a  
6                    member of Technological Crimes Learning  
7                    Institute, part of the Canadian Police College  
8                    to actually help build and develop a new  
9                    curriculum for investigations in terms of  
10                   cybercrime and cyber-related crimes.

11          Q       The Canadian Police College, by virtue of its  
12                    name at least, suggests that is training at a  
13                    national level for officers serving with the  
14                    RCMP across the country; is that right?

15          A       (AG) That is correct. We do offer training to  
16                    all police officers at all levels, municipal,  
17                    provincial and federal levels.

18          MR. MARTLAND: Okay. And I'll ask Madam Registrar to  
19                    please have your CV shown on the screen.

20          Q       Acting Sergeant, you recognize that as being  
21                    your CV?

22          A       (AG) I do.

23          MR. MARTLAND: I'll ask, please, that that be  
24                    exhibit -- I think it's 251, Mr. Commissioner.

25          THE COMMISSIONER: Yes, 251. Thank you.

1 THE REGISTRAR: Exhibit 251.

2 EXHIBIT 251: Curriculum Vitae of Cpl. Aaron  
3 Gilkes

4 MR. MARTLAND:

5 Q And, Sergeant Krahenbil, I'll next -- and I  
6 don't need the document displayed anymore.  
7 Turning to you, you're the team leader of the  
8 newly created Federal Cybercrime Operations  
9 Group, which is based into "E" Divisions -- the  
10 headquarter for the "E" Divisions being in  
11 Surrey, British Columbia; is that accurate?

12 A (AG) Yes. Yes.

13 Q And the Cybercrime Operations Group, or COG, it  
14 was launched fairly recently -- my note is  
15 April of 2020 -- with a mandate to deal with  
16 cybercrime in line with federal policing  
17 strategic priorities. Is that accurate?

18 A (AG) It is, yes.

19 Q And the goal of the group is to transition  
20 online investigations into real world police  
21 enforcement?

22 A (AG) Yes, it is.

23 Q Before assuming that role you served as team  
24 leader with FSOC, the Federal Serious and  
25 Organized Crime Unit, for five years and you've

1                   been with the RCMP since 2000?

2           A       (AG) Yes.

3           Q       And in the course of that span of time with the  
4                   RCMP you've been involved in a number of  
5                   high-profile organized crime investigations,  
6                   which include project E-Poisoned, E-Pork and  
7                   E-Pacement?

8           A       (AG) Yes.

9           Q       And those designations of E-something starting  
10                  with a P, if you could just help us understand.  
11                  Those described investigations brought in  
12                  "E" Division in British Columbia; is that fair?

13          A       (AG) It's fair.

14          MR. MARTLAND: All right. And, Madam Registrar, if  
15                  Sergeant Krahenbil's CV could please be  
16                  displayed.

17          Q       Sir, you recognize that as your CV?

18          A       (AG) I do.

19          MR. MARTLAND: Thank you. Mr. Commissioner, I'll ask  
20                  that that exhibit please be marked as  
21                  exhibit 252.

22          THE COMMISSIONER: Very well. 252.

23          THE REGISTRAR: Exhibit 252.

24                   **EXHIBIT 252: Curriculum Vitae of Cpl. Aaron**  
25                   **Gilkes**

1 MR. MARTLAND: And I'm keeping Ms. Leung busy. I'll  
2 ask next to please have displayed the first page  
3 of a PowerPoint presentation, which has been  
4 identified as appendix A.

5 Q Maybe, Sergeant Vickery, if I could ask you  
6 these questions. I know you've been involved in  
7 this. First if you could just explain, please,  
8 to the Commissioner what it is we see on screen  
9 and what the -- who's been involved in the  
10 preparation of this document.

11 A (AV) So this is the first page of a PowerPoint  
12 on virtual assets that is a joint development by  
13 Acting Sergeant Gilkes, Sergeant Krahenbil and  
14 myself. All three of us regularly provide  
15 presentations to law enforcement on virtual  
16 assets, and so we have taken what we feel are  
17 the best aspects of all of our work and combined  
18 them into one document.

19 Q All right. And we'll be spending some time on  
20 this today. We can see at the -- if you have a  
21 look at the PDF reader display there, page 1 of  
22 58. So this is a 58-page -- or a 58-slide, I  
23 should say, presentation; is that right?

24 A (AV) That's correct.

25 MR. MARTLAND: Mr. Commissioner, I'll ask that this

1                   please be marked as exhibit 253.

2                   THE COMMISSIONER: Very well. 253.

3                   THE REGISTRAR: Exhibit 253.

4                   **EXHIBIT 253: RCMP Virtual Assets Slideshow**

5                   MR. MARTLAND: And, Madam Registrar, I'll just here  
6                   and there be saying "next slide, please" as we  
7                   work our way through, and I may make reference  
8                   to the slide number if I need to do that, so  
9                   I'll give that a test right now. Next slide,  
10                  please.

11                  Q    What I'm going to ask, Sergeant Vickery, or your  
12                  colleagues, to simply, as you might do --  
13                  because I understand you've made presentations  
14                  helping to introduce the topic of virtual assets  
15                  and how does that relate to criminal  
16                  investigative work and money laundering on a  
17                  number of occasions.

18                  So why don't you simply start into that with  
19                  this first slide, and I will be asking you  
20                  questions, though, as you go.

21                  A    (AG) Okay. So -- sorry, I will begin. In terms  
22                  of bitcoin involving crimes, people rarely think  
23                  that they have encountered bitcoin, but really  
24                  the bitcoin -- well, crimes related to bitcoin  
25                  or facilitated by bitcoin or other

1                   cryptocurrencies are actually quite a bit more  
2                   prevalent than most of us know. So, please,  
3                   next slide.

4                   We can see with these news headlines that  
5                   there has been different campaigns targeting  
6                   victims throughout British Columbia. Now, these  
7                   tend to be -- when they do come into the  
8                   headlines tend to be on a smaller scale, so we  
9                   see smaller-scale scams or smaller-scale  
10                  victims, but what has to be taken into account  
11                  is the prevalence of these attempted crimes. So  
12                  it's probably not likely that anyone listening  
13                  today would not have received at some point a  
14                  phone call from someone claiming to be either  
15                  from some police agency or from the Canadian  
16                  Revenue Agency stating that they have had their  
17                  account somehow compromised or that they've been  
18                  somehow implicated in a crime and that they  
19                  would have to make payment immediately in order  
20                  to avoid going to prison.

21                  Now, payment --

22                  Q     I'm sorry, carry on.

23                  A     (AG) Sorry. Payment to avoid going to prison  
24                  typically can be requested in the form of  
25                  prepaid cards of some type or they can be made



1 of the bitcoin.

2 Q These headline examples that you've used for  
3 this third slide on the presentation, I take it  
4 those are really just examples of that --  
5 relatively smaller amounts of -- well, they may  
6 not seem that way to the victims obviously, but  
7 these aren't enormous sums of money. But  
8 individually people defrauded for some thousands  
9 of dollars and using bitcoin as a mechanism are  
10 a part of that fraudulent activity?

11 A (AG) Precisely, so a lot of these crimes  
12 actually go unreported or underreported, and  
13 part of the reason is that people are not really  
14 sure where to turn to when they do fall victim  
15 of such a crime, so -- and as well as they also  
16 may feel ashamed of the fact that they have  
17 fallen victim for this type of crime. And in  
18 the case of -- for example, if there was  
19 something related to their computer, they might  
20 think that it was more of a technological  
21 related incident rather than an actual  
22 defraud -- professional group or individual who  
23 is going out and defrauding individuals.

24 Q Thank you. I think we were about to turn to the  
25 topic, I assume, of some of the terminology.

1                   And just to situate that, these headlines -- I  
2                   think both of these headlines use the word  
3                   "bitcoin" to refer to a particular type of  
4                   cryptocurrency. As I started out, I said we're  
5                   dealing with virtual assets also sometimes  
6                   referred to as cryptocurrency. There's a number  
7                   of terms that are thrown around.

8                   And perhaps if we could go to the next  
9                   slide. And I'd appreciate the panel members  
10                  speaking to that question really of terminology  
11                  and what we're describing.

12                 MR. MARTLAND: If we could have the next slide,  
13                  please, Madam Registrar.

14                 THE WITNESS: (AV) So as you had mentioned, yes,  
15                  "virtual assets" and "virtual currency" are  
16                  often synonymous. Now, the reason why we're  
17                  using the term "virtual asset" here is because  
18                  the Financial Action Task Force has tried to  
19                  come up with a definition in order to be able to  
20                  address this, and they wanted to stay away from  
21                  the term "virtual currency" because it denotes  
22                  an actual currency. And in actual fact the  
23                  majority of the countries out there do not see  
24                  virtual -- bitcoins, say, for instance or any of  
25                  these other virtual currencies or

1                   cryptocurrencies as a currency at all. So they  
2                   wanted to get away that with term and they've  
3                   come up with something called a virtual asset.  
4                   And they've defined it as a digital  
5                   representation of value that can be digitally  
6                   traded or transferred and can be used for  
7                   payment or investment purposes.

8                   They've also said three other things. That  
9                   it can operate as a medium of exchange, which is  
10                  basically just a form of bartering that has been  
11                  around for centuries; as a unit of account -- so  
12                  no matter what the type of virtual asset it is,  
13                  it can always be valued against some other  
14                  commodity or, say, the American dollar most  
15                  commonly -- and it will always have a stored  
16                  value. So that value will change depending on  
17                  supply and demand, but it will always have value  
18                  to somebody who's willing to accept it.

19                  Next slide, please.

20                  MR. MARTLAND:

21                  Q     And in fact if we could stay on that slide, I  
22                  have one or two questions. Thank you.

23                  A     (AV) Sorry.

24                  Q     With respect to the notion that you said some  
25                  countries don't -- they resist the use of the

1 word "currency" because that maybe suggests  
2 something that would run as if it's equivalent  
3 to national currencies with a central bank  
4 authority and so forth. Is that your  
5 understanding of the resistance to that  
6 terminology?

7 A (AV) Yes, exactly. It's a central bank issue,  
8 digital currency.

9 Q So I take it that one of the things that's  
10 distinctive about virtual assets is the fact  
11 that they're not tied to a central bank  
12 authority which either decides, here's our  
13 monetary policy and decisions about circulation  
14 of their currency, or, for that matter, tying it  
15 to an established currency like the US dollar?

16 A (AV) Yes.

17 Q Are -- in general terms, and if you need  
18 specifics that's fine, are there virtual assets  
19 that are tied to physical commodities? We think  
20 of the old notion of a currency that might be  
21 tied to a value in gold or some other physical  
22 commodity.

23 A (AV) Absolutely there are. Also there's  
24 something that's called stable coins. We talk  
25 about them a little bit later on in the

1 presentation as we go into the different kinds  
2 of cryptocurrencies there are. Is it okay if I  
3 wait until then?

4 Q It is. That's fine, and we'll come to that. I  
5 wonder if I could just also ask this question  
6 since we see the terminology about "virtual  
7 asset." Does the term "asset" also have a  
8 particular implication for law enforcement?

9 A (AV) Well, certainly if it's considered to be a  
10 proceeds of crime or offence-related property,  
11 then it would.

12 Q We can go to the next slide, please. Thank you.

13 A (AV) Okay. So there's two different types of  
14 virtual assets that exist. There's something  
15 called non-convertible, which means that it only  
16 has value within the domain in which it is being  
17 used. It's seen often in online gaming, such as  
18 the World of Warcraft. If we wanted to take  
19 that into a real life scenario it would be very  
20 similar to Canadian Tire money. So there's  
21 value within Canadian Tire, but we try to keep  
22 it outside of Canadian Tire and nobody is really  
23 willing to be -- able to accept it.

24 And then there's something called  
25 convertible. So there's two kinds of

1 convertible virtual assets. There's centralized  
2 and there's decentralized. So "centralized"  
3 just means that there's a single administrative  
4 authority. Now, we have the example there of a  
5 Second Life virtual world, which is an online  
6 gaming world, and they use something called  
7 Linden money and -- where the players can  
8 purchase real estate and various commodities and  
9 assets within this world, and then they can  
10 exchange those funds for real fiat currency out  
11 in real -- in the real world.

12 There's also centralized cryptocurrencies  
13 that exist out there or assets, and Acting  
14 Sergeant Gilkes will be speaking about some of  
15 those later. And then we have decentralized.  
16 So this means that there's no single  
17 administrative authority, there's no central  
18 bank overseeing the issuance of these virtual  
19 asset, no oversight whatsoever, and they operate  
20 purely on a peer-to-peer basis.

21 So virtual currencies are assets which are  
22 convertible, meaning that they can convert from  
23 cryptocurrency or currencies into fiat; are  
24 decentralized, so have no single oversight,  
25 administering oversight; and use something

1                   called cryptography, which is a method to be  
2                   able to secure the transactions, are known as  
3                   cryptocurrencies.

4           Q        You used the term "converting to fiat." And  
5                   just so we're clear about that terminology,  
6                   that -- does that describe what most of us would  
7                   just simply think of as money but, in other  
8                   words, Canadian or American dollars or  
9                   British pounds, but real world cash at hand,  
10                  that sort of idea?

11          A        (AV) Exactly. Central-bank issued currencies.

12          Q        Okay. Thank you. We'll go to the next slide,  
13                   please.

14          A        (AG) This slide speaks to the overall -- well,  
15                   the overall importance of cryptocurrencies, at  
16                   least in 2017. So this is a snapshot of the  
17                   value, the approximate market capitalization,  
18                   which is essentially the value of each share, or  
19                   in this case each coin, multiplied by the number  
20                   of coins in circulation give you the overall  
21                   value of the particular cryptocurrency. And we  
22                   can see this was -- in 2017 before there was  
23                   a -- well, a considerable rise in the value of  
24                   bitcoin. I think, for example, the year it  
25                   reached close to \$20,000. But we can see here

1                   that bitcoin at that time was -- had an  
2                   approximate value of \$20 billion overall, and it  
3                   was news back then for there to be  
4                   10 cryptocurrencies with a market capitalization  
5                   of over \$100 million, which seems rather  
6                   important. But if we jump ahead now to the next  
7                   slide, please. And we take a snapshot of the  
8                   top 10 cryptocurrencies in 2020, we can see that  
9                   the market capitalizations have increased  
10                  dramatically.

11                  So we can look first at bitcoin, which now  
12                  has a market capitalization of approximately  
13                  \$300 billion. I mean, yes, we are taking into  
14                  account that there are more of them in supply --  
15                  or actually available, but we can actually take  
16                  a look at all of other top 10 and we can see  
17                  that there's been exponential growth, so much  
18                  more than ten times the value that we had seen  
19                  in 2017.

20                  Now, this should give a clear idea that  
21                  these cryptocurrencies have actually reached a  
22                  large percentage of individuals in the world and  
23                  you can see their importance simply based on the  
24                  amount of funds that they generate and that they  
25                  hold in terms of value.



1           Q     You mentioned that -- the year 2017, and I take  
2                   it that's actually quite a notable year with  
3                   respect to at least the value of the bitcoin in  
4                   particular. That was the banner year so far  
5                   with a bit of a footnote beside that to ask  
6                   whether we're presently coming up on the same  
7                   sort of dynamic right now, I gather.

8           A     (AG) That is correct. So that was at the time  
9                   when bitcoin had reached -- I think it was  
10                  \$20,000 in December. I believe the value of --  
11                  it currently is not very far from there.  
12                  There's all sorts of possible reasons for that  
13                  to happen, but I'm not really sure exactly what  
14                  in each circumstance causes the increase.

15          Q     And if it's the case that 2017 and 2020 look to  
16                  be sort of relatively peaks, have there been  
17                  valleys in between? Has there been in general  
18                  terms some ups and downs with respect to the  
19                  cost in particular bitcoin?

20          A     (AG) Yes. There's actually been considerable  
21                  ups and downs, I suppose we can call it. We've  
22                  seen -- I suppose in 2018 we had seen bitcoin be  
23                  turned down to I suppose around \$10,000 in  
24                  value, so lost close to half, I believe. I'd  
25                  have to look at the exact capitalization to know

1 in 2018. But there has been considerable  
2 fluctuation with value of bitcoin throughout its  
3 history since its inception.

4 Q And this -- and I think both the previous slide  
5 and this slide show a list of really the top 10.  
6 Could you give us a sense of how many virtual  
7 currencies are out there?

8 A (AG) There are thousands. There are thousands  
9 of virtual currencies, some of which have their  
10 own blockchain, which we will discuss later, and  
11 some of which are operating on an existing  
12 blockchain, for example, operating on the  
13 Ethereum blockchain. Those are considered  
14 tokens, but a virtual asset nonetheless.

15 Q And these two slides, I think both of them  
16 suggest a significant dominance when one  
17 compares bitcoin to its competitors. Is that a  
18 fair conclusion to draw?

19 A (AG) Yes. And this might be due to the  
20 infrastructure that's already in place. It  
21 might be due to the popularity and the  
22 overall -- I don't really want to the call it  
23 advertising, but the fact that bitcoin appears  
24 often in the new media and people speak about it  
25 in general. It breeds a certain familiarity

1                   with the coin itself and that familiarity -- and  
2                   there's also a lot of information available on  
3                   how to actually transact with bitcoin and much  
4                   less available for the other cryptocurrencies.  
5                   So it's a lot easier to do the necessary  
6                   research to actually purchase your own  
7                   cryptocurrencies or become a cryptocurrency  
8                   hobbyist using bitcoin.

9                   Q     So I guess to some extent maybe that's a bit  
10                   like Kleenex or Xerox or one of these companies  
11                   that achieve such -- "currency" maybe is the  
12                   wrong word, but such prevalence in the popular  
13                   discourse that people might use bitcoin when in  
14                   fact technically it's a different cryptocurrency  
15                   that could be at issue or at least described?

16                   A     (AG) That is correct.

17                   Q     Are there any -- I may be taking you a little  
18                   out of sequence here as I ask these questions.  
19                   Are there any virtual currencies that are  
20                   actually tied to or managed by a national  
21                   banking authority, like a central banking  
22                   authority or a country?

23                   A     (AG) In terms of a country, I suppose -- I'm not  
24                   sure if Sergeant Vickery might be better placed  
25                   for that particular question.

1 (AV) So as far as I know, not yet; however,  
2 there are a lot of countries out there looking  
3 at the proposal. China is very close to issuing  
4 one and I believe they're about to launch a  
5 lottery where they're going to give out  
6 approximately \$1 million in these digital assets  
7 to citizens to be able to use.

8 Canada even is part of a working group  
9 right now with some of the other countries to  
10 identify the best practices and approach to the  
11 potential. They are not looking at developing a  
12 digital -- a central bank digital currency  
13 currently here in Canada but are exploring that  
14 option in the future. I believe Venezuela has  
15 also looked at doing this. So it is something  
16 that many countries out there see the value in.

17 Certainly the blockchain technology  
18 provides innovation and transparency that's  
19 never been available before. So, you know, in  
20 my opinion I won't be surprised if this becomes  
21 more of a common move in the future.

22 Q Thank you. I think we're in a position to move  
23 to the next slide. This is an important heading  
24 obviously because people wonder, they hear this  
25 description of the blockchain. If you could

1 help us to please understand exactly what that  
2 is and how it operates.

3 A (AG) Sure. Absolutely. So in order to  
4 properly understand bitcoin you need to  
5 understand the technology that it's actually  
6 built on. Now, it's built on something called a  
7 blockchain, when in actual fact the  
8 blockchain is more like a database. Now, it's  
9 an innovative database in that everything added  
10 to the database cannot be modified, deleted,  
11 removed in any such way -- in any which way.

12 So if we are talking specifically about  
13 bitcoin and how it works on a blockchain, we  
14 could possibly relate it to either an Excel  
15 spreadsheet or an open ledger, accounting  
16 ledger, which is actually distributed to anyone  
17 who requires or who would like to have a copy of  
18 it.

19 Now, if we assume that each page of the  
20 ledger has space for about 100 entries and that  
21 each bitcoin transaction, so a transaction  
22 sending money to and from individuals, accounts  
23 for one entry, we can fill those entry fields  
24 with one transaction each up until we get to  
25 100, which would fill the page. Now, I'm simply

1                   using a number 100 because it's easier for -- in  
2                   terms of reference. But once this has been  
3                   filled, this page becomes, well, part of the  
4                   block. So what happens are that there are  
5                   individuals who are processing these  
6                   transactions and these transactions will be  
7                   completely processed and then they'll become a  
8                   block, so a page that's locked and cannot be  
9                   changed at any time in the future.

10                   Now, once that page a locked it is  
11                   translated into a cryptographic hash, which  
12                   means -- sort of like a numerical representation  
13                   of all of those transactions. That way if any  
14                   of those transactions are changed at any time in  
15                   the future, even by one number, we will see that  
16                   the hash itself will actually change and then we  
17                   will know that there's been a change, but -- we  
18                   may not know exactly what has changed, but we  
19                   know that it's not the same page that we were  
20                   working with when those transactions were -- the  
21                   word is "confirmed" or "verified."

22                   Now, those transactions are being processed  
23                   by individuals or groups who we call miners.  
24                   And those miners basically solve cryptographic  
25                   hashes in order to add each of those

1 transactions to a block.

2 Now, as a reward for what they do they are  
3 paid transaction fees. Those transaction fees  
4 are actually paid by the individuals who are  
5 sending the funds. It may sound strange, but if  
6 we think it into -- if we think about it in  
7 terms of PIN processing by maybe Visa or  
8 Mastercard or Interac, the same thing is  
9 happening only it's all occurring under one  
10 central body, one central entity, and it's  
11 typically the vendor who's paying fees for the  
12 transaction itself. So basically it has just  
13 taken -- it has just reversed or flipped the  
14 side of where the transaction fees are coming  
15 from.

16 Now, what a miner --

17 Q Let me just perhaps --

18 A (AG) Sorry.

19 Q Sorry, just -- this question just occurred to  
20 me. When you describe this in a very  
21 decentralized environment, how is a decision  
22 made as to who gets the next transaction, so to  
23 speak? Which miner -- I don't know if there's  
24 competition or if that's, like, a lottery or how  
25 it is that those get sent around to different

1 miners.

2 A (AG) Well, there actually is a competition  
3 that's built into the platform itself, built  
4 into the technology. Now, the -- basically a  
5 transaction or a block is added every  
6 ten minutes and it has to function like this in  
7 order for the distribution of the coins  
8 themselves because when a block is solved, or  
9 when a block is added, the miners are paid with  
10 newly minted bitcoins. And that's kind of why  
11 they're called miners; right? Because they --  
12 these coins didn't exist before or they weren't  
13 in circulation before, but now they're being  
14 distributed through the discovery of a new  
15 block.

16 Now, in order for the blocks -- because  
17 there are a finite number of bitcoins that  
18 exist. There's -- or that will exist. There's  
19 slightly over 21 million, I believe, bitcoins  
20 that will some -- exist in the future.

21 Now, in order to make sure that there's  
22 enough bitcoins that are distributed at a proper  
23 pace it has to take approximately 10 minutes for  
24 each block to be solved. Now, what happens is  
25 that depending on how powerful or how many



1 miners are working to solve these blocks, the  
2 difficulty of solving the blocks will be  
3 adjusted. And when I say "difficulty," I mean  
4 that the hash has to reach, give or take, a  
5 certain number that's created by the network,  
6 that's created by the software itself.

7 Now, the first miner to reach that number  
8 is awarded the block. So he's awarded the  
9 payment for not only the transaction fees but  
10 also the initial coins that are uncovered with  
11 the solving of the block. So it is a  
12 competition as to who can solve that equation  
13 the fastest and who can add that block of  
14 transactions to the blockchain the fastest.

15 (AV) If I may just cut in here is just to  
16 mention an additional incentive for them is the  
17 transactions fees. So every time somebody  
18 conducts a transaction dealing with bitcoin they  
19 have to add a transaction fee to it. Now,  
20 that's not dependent on the actual size of the  
21 transaction but rather the amount of addresses  
22 that are involved in that. So when there's high  
23 demand for bitcoin transactions, there can be  
24 several transactions all occurring  
25 simultaneously. Now, in order to fill this

1                   block every ten minutes it can hold  
2                   approximately 1 megabyte of data, which works  
3                   out to about 2,000 transactions. And so really  
4                   it's up to the miner to scoop up those -- group  
5                   of 2,000 transactions to be able to solve this  
6                   computational mathematical puzzle in order to  
7                   create that block.

8                   And there -- in order to incentivize them,  
9                   in order to grab your transaction to get it  
10                  solved within that first block and hopefully be  
11                  validated within that first 10 minutes, you want  
12                  to be able to increase that -- the value of that  
13                  transaction fee so that they are more willing to  
14                  grab yours instead of having it sit in  
15                  cyberspace for, you know, two, three, four, five  
16                  blocks down the road before your transaction is  
17                  actually validated and is added to the  
18                  blockchain.

19                Q     Go ahead.

20                A     (AG) If we're thinking in terms of efficiency,  
21                  we're looking at the potential for three to  
22                  seven bitcoin transactions per second. Now, if  
23                  we scale that and in comparison we're looking at  
24                  about more or less 200 transactions per second  
25                  for PayPal and we're in the tens of thousands

1 per second for a platform like Visa or  
2 Mastercard in terms of processing transactions.

3 So it doesn't scale anywhere near that of  
4 those other, I would say, remote or digital  
5 payment systems structure out there.

6 Q You described the ledger and say that that's a  
7 public ledger. Do I have that right?

8 A (AG) Yes. So the blockchain -- or the bitcoin  
9 blockchain, I should say, is a public ledger.  
10 Not all cryptocurrencies have a public ledger,  
11 but in the case of blockchain it is. And there  
12 are tens of thousands of what are considered --  
13 or what are called nodes in the world, which  
14 actually keep track of all of this -- of the  
15 entire blockchain. Which means that every  
16 transaction since its inception in 2009 is  
17 recorded and kept on these tens of thousand of  
18 nodes. So in order -- that creates considerable  
19 redundancy.

20 So in order for the entire network to go --  
21 well, for the -- for blockchain or for bitcoin  
22 to go down, the entire blockchain would have to  
23 be wiped out at the same time on all of the  
24 computers or nodes in the world. So -- those  
25 are tens of thousands, so the chances of that

1                   happening are relatively limited.

2                   So it does create challenges, which we will  
3                   discuss going further, but that would, well,  
4                   speak to the decentralization of the blockchain  
5                   itself.

6           Q       You describe the -- Acting Sergeant Gilkes, you  
7                   described it as being a ledger and the  
8                   information on it cannot be modified or deleted,  
9                   so I take it that's a permanent ledger and one  
10                  that does not admit of being forged or  
11                  manipulated because of that feature?

12          A       (AG) That is correct. So the miners themselves  
13                  in addition to processing the transactions --  
14                  the new transactions, their -- part of their  
15                  assignment is also to go back and verify each  
16                  and every block that's ever been added to the  
17                  blockchain as they are verifying or as they are  
18                  completing and processing the new transactions.  
19                  So if there is any type of change, if there is  
20                  any type of modification or mismatch, then they  
21                  know that there's something wrong in the block  
22                  and that they cannot go forward with confirming  
23                  or adding new block to the chain.

24          Q       What information is on the public ledger?

25          A       (AG) In terms of information on the public

1 ledger, we will see the date and time of the  
2 transactions. We'll see the accounts that the  
3 bitcoins were sent from and the account that the  
4 bitcoins were sent to in addition to the  
5 transaction number and the amount of coins that  
6 were actually transacted at that time. We'll  
7 see what that actually looks like in real life a  
8 little bit -- in a couple of slides, but there's  
9 actually a considerable amount of information in  
10 relation to each transaction, which is available  
11 publicly with simple open source software that  
12 allows for blockchain exploration.

13 Q You describe -- maybe you could comment on this:  
14 to what extent is the information kept in a  
15 manner that permits anonymity? How anonymous is  
16 it to be -- let's focus on bitcoin for this  
17 question. How anonymously can one engage in  
18 these transactions in terms of a ledger that  
19 maintains a store of information and detail  
20 about transactions?

21 A (AG) Well, the term "pseudo-anonymous" has been  
22 used often with blockchain, or pseudonymous,  
23 meaning that almost all information is actually  
24 available publicly with the exception of the  
25 identity of the person who actually conducted

1                   the transaction and the location. So I kind of  
2                   compare it to your using ATM machine and leaving  
3                   your transaction slip behind you. So the person  
4                   would be able to see how much money you may have  
5                   withdrawn, they may actually -- they'll be able  
6                   to see from which bank you've actually completed  
7                   your transaction and maybe some information  
8                   pertaining to the accounts that you used, but  
9                   they might not know who you are, your actual  
10                  name and residence. So we do consider that to  
11                  be pseudo-anonymous.

12                         Now, having this information available, I  
13                         can speak in terms of law enforcement firsthand,  
14                         can very much aid, for example, investigators.  
15                         And what I mean is this is information which we  
16                         would typically have to complete a production  
17                         order in order to obtain from a bank or  
18                         financial institution, whereas here we could  
19                         simply go publicly and confirm that a  
20                         transaction has actually occurred. And  
21                         especially, I think, in relation to transactions  
22                         may have occurred outside of the Canadian  
23                         jurisdiction or overseas, this is information  
24                         with -- which can be requested but we'd have to  
25                         use mutual legal assistance treaties and other

1                   tools, which can greatly delay an investigation  
2                   and potentially hamper the outcome. So having  
3                   this information available at an investigator's  
4                   fingerprints can accelerate and really help an  
5                   investigation.

6           Q       Just to pick up on that, when you describe that  
7                   it's -- it provides relevant and useful  
8                   information but not necessarily the identity of  
9                   the person doing it, I take it in sort of  
10                  analogous terms and in terms of the  
11                  investigative value, this isn't the person's  
12                  dropped their ID at the crime scene or left  
13                  their fingerprints on the holdup note so much as  
14                  they've left behind some value -- some valuable,  
15                  maybe circumstantial evidence that can connect  
16                  with other information to help you figure out  
17                  who's behind something but not all the way there  
18                  to identifying that person?

19          A       (AG) Precisely. This information would have to  
20                  be used in conjunction with -- I call it good  
21                  old fashion policing in order to put the pieces  
22                  together and actually identify who may have been  
23                  responsible for whatever crime may have occurred  
24                  and to confirm the crime that may have actually  
25                  occurred itself.

1           Q     I've taken you already offscript, but why don't  
2                    you return to the slide we have there, please.

3           A     (AG) Oh, sure.  Actually, I believe we're ready  
4                    to move to the next slide.  Okay.  As I  
5                    mentioned before that there are miners working  
6                    as individuals or as groups who are paid to  
7                    complete transactions for the bitcoin network.

8                            Now, this is a headline from approximately  
9                            a year and a half ago and this is an investment  
10                           from a cryptomining farm or a bitcoin miner.  
11                           Now, it's kind of, I guess, difficult to see  
12                           from this photo, but this individual is actually  
13                           handling computers.  So these are  
14                           application-specific computers which are created  
15                           with a sole purpose of mining bitcoins or other  
16                           cryptocurrencies.  They are very, very powerful  
17                           computers but they only do one thing.

18                                    Now, these computers generate an enormous  
19                                    amount of heat and require an enormous amount of  
20                                    electricity in order to function.  So this  
21                                    company created a farm -- a crypto farm in  
22                                    Quebec -- in Sherbrooke, Quebec.  Now, one of  
23                                    the reasons -- and it's one of many farms in  
24                                    Quebec and in Canada, but particularly in  
25                                    Quebec.  Now, one of the reasons is -- well,



1                   like I mentioned before that these machines  
2                   generate considerable amount of heat. So the  
3                   climate in Quebec is colder than many and also  
4                   the electricity in Quebec is very inexpensive,  
5                   so as a result many of these companies have  
6                   moved there. And there's also little regulation  
7                   in terms of -- well, at least regulation that  
8                   would stifle the develop and growth of the  
9                   cryptocurrency market in Quebec.

10                   So the takeaway here is that there is  
11                   \$250 million being invested in this type of  
12                   facility. We can assume, then, going forward  
13                   that the investors would expect an exponential  
14                   return in their investment and they are not  
15                   expecting to simply flush their money down the  
16                   toilet. So if there are groups and individuals  
17                   investing this type of money, we can -- into the  
18                   infrastructure, the bitcoin infrastructure, we  
19                   can expect bitcoin to continue to grow or  
20                   continue to be prevalent.

21                   Q    I don't want to draw too much from one person --  
22                   of one fellow in a toque, but this seems to be  
23                   not a hobbyist's pursuit, someone with a  
24                   computer who decides they're going to be a  
25                   miner. It seems, the nature of what you've

1                   described, pretty significant computer power and  
2                   some capacity to be competing and succeeding in  
3                   the competition to be a bit farmer; is that  
4                   accurate?

5           A       (AG) Correct.  If we think in terms of -- well,  
6                   basically 2009, 2010, I suppose up until about  
7                   2012 or so, if you had a very powerful computer,  
8                   you could compete, but at this point these  
9                   computers and the heavy investment in some of  
10                  these computers costs them tens of thousands of  
11                  dollars.  It would not be likely that if you  
12                  were to attempt to solve a block yourself with  
13                  one computer that you would actually be  
14                  successful.

15                         There is a way of joining a pool, basically  
16                         a pool of resources which can work together in  
17                         order to solve the cryptographic hashes and add  
18                         the blocks, but that would be -- in terms of  
19                         opinion only, I'm not really sure that it would  
20                         cover the electricity that it would cost to  
21                         actually run this type of machine.

22                                 Next slide, please.

23           Q       Next slide.  Thank you.

24           A       (AG) Thank you.  So as I was saying before, this  
25                   would be the type of information that you could

1                   recuperate or simply access on the blockchain.  
2                   So this would be taken from blockchaininfo.com.  
3                   And this is actually a transaction that I myself  
4                   conducted with one of my wallets back this 2017.

5                   Now, this is a simple deposit via a bitcoin  
6                   ATM. Now, the, I guess, rectangle above would  
7                   be the transaction with the amount of bitcoin  
8                   and below you'd see the translation of the  
9                   amount of money that was actually transacted.  
10                  Now, the hash that you can see there would be  
11                  actually the transaction number and below that  
12                  you would see the wallet -- or sorry, the  
13                  address, I should say, that the bitcoins came  
14                  from. And the on the right-hand side you see  
15                  there's kind of a green globe there, and that's  
16                  where the money or the bitcoin was deposited to.  
17                  So that actually is the account that was under  
18                  my control at that time, and I should mention,  
19                  please, no one send me bitcoin.

20                  Q    Wait a sec. I think you do want them sending it  
21                      to you, just not taking it away. So this will  
22                      be quite inexact, but am I right to say, then,  
23                      as we look at this, sort of is a ledger of a  
24                      transaction at one level. What's going on is  
25                      that the -- if we look at the blue globe on the

1 left side would be akin to saying this is from,  
2 let's say, a CIBC account in Vancouver. And  
3 then with an arrow to the right going to a Bank  
4 of Montreal account in Saskatoon. And the hash  
5 at the top would be sort of functionally  
6 equivalent to -- I don't know what that would be  
7 equivalent to. Would that be sort of like a  
8 transaction number?

9 A (AG) Correct. It would be the transaction  
10 number relating to the block that it came from.  
11 And in this case it was likely that the -- where  
12 the coins came from would be the exchanger who  
13 actually manages the ATM that I was dealing  
14 with.

15 Q Okay. Yeah.

16 A (AG) We can see that there is a date and time  
17 and there's an amount as well as the fee that  
18 was paid out in order to complete the  
19 transaction.

20 Q And all of these different displays of the hash  
21 and such and the addresses have ellipses at the  
22 end, so I take it they're quite a long number  
23 and letter series, aren't they, that are  
24 involved?

25 A (AG) Yes, they are. We'll discuss a little bit

1                   about that, I suppose, when we go forward and  
2                   speak about private keys and public keys and  
3                   things like that.

4           Q        Good.  Shall we move to slide number 11?

5           A        (AG) Sure.

6                   (AV) Sorry.  So unlike cash, which is  
7                   completely traceless, the blockchain -- or at  
8                   least the bitcoin blockchain will allow us to be  
9                   able to see a transaction most of the -- the  
10                  cryptocurrency -- or sorry, a history of most of  
11                  the cryptocurrency transactions that have ever  
12                  occurred.  So from a law enforcement perspective  
13                  this provides us an ability to trace and follow  
14                  the flow of funds to an extent that's just not  
15                  currently not available to us with the  
16                  traditional banking system.

17                  So currently, you know, if grounds permit,  
18                  then we can obtain a production order and we can  
19                  go to a bank and we can obtain production order  
20                  results which identify account information and  
21                  account history for a suspect of our  
22                  investigation.  Usually, you know, this can  
23                  cause some time delays where we can wait up to  
24                  90 days for this information in which time we  
25                  can analyze and assess it and maybe identify

1 co-conspirators or further accounts and  
2 different banking organizations that we can then  
3 follow up with additional production orders.  
4 And all of this takes time and process to be  
5 able to get there, whereas we can look at the  
6 blockchain and we can get a pretty good  
7 indication of the flow of the transactions from  
8 that.

9 As Acting Sergeant Gilkes had mentioned,  
10 that -- sorry, I lost my train of thought there  
11 for a second. I'll just go back to --

12 Q Maybe I can ask you because one question of  
13 course occurred to me as we go through this.  
14 You describe that in the conventional banking  
15 situation, the police investigating something,  
16 they don't simply place a phone call to the --  
17 to a federal bank, let's say, and suddenly  
18 receive the same day the information. There's a  
19 legal regime that requires prior judicial  
20 authorization, so an application, you mentioned  
21 a production order under the Criminal Code,  
22 where there's a standard that has to be met.  
23 It's not simply we're interested, but we  
24 actually have a reasonable basis to believe that  
25 we may have evidence that emanates from

1 information that -- in this example, that the  
2 bank has.

3 So I take it that here we're dealing with  
4 something entirely different. You don't have to  
5 be satisfying a ground of -- reasonable grounds  
6 to believe that you may have evidence related to  
7 a crime; you don't need to have a judicial  
8 officer approving a warrant or production order?

9 A (AV) So that depends. The information that's  
10 available to us on the blockchain through open  
11 source technology or through using these  
12 aftermarket software tools, we can do an  
13 analysis of the transactions and get a history  
14 of the movement and flow of that -- funds.  
15 These aftermarket software tools that cost money  
16 that law enforcement are able to purchase also  
17 will help provide links to criminality, links to  
18 risky addresses, exposure so the darknet, to  
19 mixing services, which is a third-party money  
20 laundering service which we'll talk about a  
21 little bit later in the testimony.

22 But that's what these tools provide us.  
23 However, they still will not identify who the  
24 holder of that account is. And in order for us  
25 to get that information, we then -- we will have

1                   to follow the trace until such time it goes to  
2                   an on ramp or an off-ramp. And when I say that  
3                   I'm talking about the methods of cashing out and  
4                   converting it over to a regular currency, so --  
5                   such as through an exchange. We'll talk shortly  
6                   about the type of information -- how exchanges  
7                   are structured and the type of information that  
8                   they get. But at this point, if we can see a  
9                   transaction going to a exchange, then we can go  
10                  forward and get a production order with legal  
11                  authorization from a judge because we have  
12                  reasonable grounds to believe an offence has  
13                  occurred, and then we can get that information.

14                  (AG) I would like to add that the tools are  
15                  not an exact science. So we're thinking about  
16                  heuristics here. So there is clustering,  
17                  basically trying to attribute multiple  
18                  transactions to the control of one or several  
19                  individuals. There's also some properties  
20                  inherent in the blockchain which allow for  
21                  the -- I would say, which aid in providing a  
22                  location for where a transaction may have  
23                  occurred. But a lot of, I would say -- I don't  
24                  want to call it guesswork because it is educated  
25                  guesses, but based on information which is



1 collected in the clearnet, the darknet,  
2 information -- circle information, reports from  
3 police, reports in -- well, in journalistic  
4 reports, will provide information that will help  
5 to attribute ownership or attribute usership of  
6 particular addresses, but, like I mentioned, not  
7 an exact science and regular policework has to  
8 be done in collaboration.

9 Q So the slide that we have on display talks about  
10 aftermarket software tools. I see three dollar  
11 signs. If it was a restaurant review, this is a  
12 fancier restaurant, I take it. And we see a  
13 description on the slide, which I don't need to  
14 read out, but if you could give us a sense of  
15 what this describes and then how it is that law  
16 enforcement and in particular the RCMP engages  
17 with these sorts of tools and providers.

18 A (AV) Sure. So I have the three dollar signs  
19 there because yes, they don't necessarily come  
20 cheap. But there are companies out there that  
21 do an analysis of the blockchain, and as Acting  
22 Sergeant Gilkes had mentioned, be able to  
23 attribute and cluster addresses together and  
24 link them to criminality such as, you know,  
25 originating or passing through darknet or

1 related to other cryptocurrency addresses that  
2 have been linked to hacks or frauds.

3 And so we have specialized resources within  
4 law enforcement that are trained to be able to  
5 utilize these software tracing tools, to be able  
6 to do an analysis of that information. Again,  
7 they can identify IP addresses, potentially.  
8 While this will not identify who the holder of  
9 that have account is, it does usually permit us  
10 the ability to be able to use judicial  
11 authorization to be able to gain access to  
12 further information from the exchanges or the  
13 third-party service providers who facilitated a  
14 transaction through their exchange.

15 Q Could you give the Commissioner a sense of who  
16 the big players are in this area and whether  
17 they are based in or operating in Canada as  
18 opposed to elsewhere, and for that matter, how  
19 they are structured? Who's -- is it a company  
20 that's behind it, et cetera?

21 A (AV) So the largest -- the software companies,  
22 at least for Canadian law enforcement, tends to  
23 be Chainalysis and CipherTrace. The National  
24 Cybercrime Coordination Centre in Ottawa, which  
25 is the National Police Services, acquired

1                   several licences of each of these -- from each  
2                   of these companies to be able to a support  
3                   Canadian law enforcement at a municipal,  
4                   provincial and federal level.

5                   There are other software companies that do  
6                   exist, such as a Elliptic, although that is a  
7                   company that is used more commonly in Europe. I  
8                   know the UK tends to use them quite a bit, but  
9                   here in Canada we typically rely on CipherTrace  
10                  and Chainalysis.

11                 Q   And are those -- and are those sort of providers  
12                   that are looked to by law enforcement to offer  
13                   sort of tools and software to do that work, or  
14                   are they actually really -- to some extent is  
15                   worker analysis outsourced to those providers?

16                 A   (AV) So they would post these servers with all  
17                   the information, and then the law enforcement  
18                   agencies will utilize their data from -- or  
19                   their platform basically to be able to do this  
20                   analysis, and then based on the information  
21                   that's a gathered from various law enforcement  
22                   entities that are using their tools they're able  
23                   to attribute certain addresses to criminality  
24                   and be able to come up with some trends on how  
25                   cryptocurrency is being utilized. So

1                   CipherTrace and Chainalysis very often will  
2                   analyze this data and put out reports such as  
3                   the 2020 Chainalysis report and there's a  
4                   CipherTrace one as well, will do a quarterly  
5                   report, I believe.

6                   Q    Does it makes sense that we move to the next  
7                   slide, number 12, which is in entitled  
8                   "Public/Private Key Pairs," to understand more  
9                   about what the key pair describes?

10                  A    (AG) Okay.  So we'll be getting into bitcoin  
11                   wallets.  So basically everything that I've  
12                   discussed before on the blockchain, what does an  
13                   individual see when they actually create their  
14                   own bitcoin account, I suppose you can call it,  
15                   would be when they create their own wallet they  
16                   are given a private key.  So basically the  
17                   private key is the one that you can see there at  
18                   the bottom written in red, and it's very, very  
19                   long, and that's important because it's similar  
20                   to having a password.  And this password allows  
21                   you access to whatever bitcoin are stored in  
22                   whatever addresses are associated with this  
23                   private key.  So it allows you to spend it.

24                                Now, it's enough to simply see it, or to  
25                   see what's called a QR code.  So you can see

1                   that there's something that looks like a barcode  
2                   on the right-hand side. There's also an  
3                   associated code with a private key. So anyone  
4                   who sees that can take a picture of it, or can  
5                   simply memorize the numbers, can actually  
6                   rebuild the wallet that this is actually  
7                   associated to and then use whatever coins are  
8                   associated to it.

9                   So it's, I guess, considered an enhanced  
10                  password because you can actually use this or  
11                  several people can share the same private key  
12                  and all have access to the same account and all  
13                  have the ability to spend the same coins that  
14                  are associated to the same wallet. Now, when  
15                  I'm talking about a wallet, I'm referring to  
16                  actually the public keys that are associated.  
17                  So public keys can be considered account numbers  
18                  or accounts that are associated to the private  
19                  key which would be in the wallet itself.

20                  Now, the public keys are where you would  
21                  actually send or receive the bitcoins  
22                  themselves, and they're actually not necessarily  
23                  private. So this is a key that you don't mind  
24                  having it shared with other individuals because  
25                  they can use it as your account number, for

1                   example, to send funds to. So you can sort of  
2                   consider it, like I said, an account number or,  
3                   as we can see here, any email address for  
4                   accepting e-transfers. So that would cover  
5                   that.

6                   Q    And just to pick up on that so I have the point.  
7                   If you lost your public key that's not the end  
8                   of the world. That's -- people may or may not  
9                   circulate it widely, but there's nothing that  
10                  puts you at risk of having your account emptied,  
11                  so to speak. But losing the private key could  
12                  give rise to that risk that someone else then  
13                  has effectively the ability to move that bitcoin  
14                  or money around?

15                  A    (AG) Right. And like I mentioned before, it's  
16                  really enhanced. So it's not quite -- losing  
17                  your private key is not exactly like losing your  
18                  wallet because if you do lose your wallet, well,  
19                  whoever finds it can use it. But in the private  
20                  key, if I have seen your private key or I have  
21                  taken a picture or somehow recorded the  
22                  information from your private key, even though  
23                  you may still physically be in control of  
24                  whatever device this may be stored on, because I  
25                  have taken that picture, I can actually spend

1                   your bitcoins.

2                   Q     Thank you.

3                   A     (AG) So next slide, please. Okay. Now, in term  
4                   of managing your cryptocurrencies, and I had  
5                   mentioned before the creation of wallets. And  
6                   so as it says there:

7                             "Digital wallets are hardware or software  
8                             that manage keys, addresses, and  
9                             transactions."

10                   Now, you need to create a wallet. And there's  
11                   several different types of wallets that we'll  
12                   talk about briefly, the first one being an  
13                   online wallet. Now, an online wallet is, well,  
14                   I suppose a wallet which has the least amount of  
15                   control for the person who's actually creating  
16                   the wallet. Now, these tend to be held by  
17                   exchangers. So, now, you would simply log into  
18                   an exchanger, provide your personal information  
19                   and create an account.

20                             Now, this account would then give you some  
21                             public keys or addresses or account numbers  
22                             basically to send funds to or to send bitcoins  
23                             to, but with that being said, the exchanger will  
24                             keep control of your private key. So it's much  
25                             like depositing your money in the bank. So when

1                   you deposit your money in the bank, they have  
2                   total control of your funds. They can do pretty  
3                   much whatever they want with your money, and  
4                   it's the same thing with an exchange. So they  
5                   will keep your private key -- well, they will  
6                   keep control of the private key and just allow  
7                   you to spend funds that have been deposited with  
8                   their business or with their exchange.

9                   Next we have desktop and mobile wallets,  
10                  which are essentially the same thing only  
11                  portability is different. Now, these wallets,  
12                  these can be used to -- well, this is software  
13                  that is downloaded and it's used to generate  
14                  wallets on your own device. So you keep control  
15                  of your keys personally, so your private keys  
16                  and your public keys, and you have full control  
17                  over your transactions. These ones, the mobile  
18                  wallet, the desktop wallet and the online  
19                  wallets, are very -- tend to be very fast  
20                  because they are what you would call hot  
21                  wallets, so meaning that they are wallets where  
22                  the private key is or has been online, and they  
23                  can be used to conduct transactions relatively  
24                  swiftly.

25                  Now, in terms of security, a wallet being



1                   held -- an online wallet being held at an  
2                   exchanger, that is -- depending on how you look  
3                   at it, it can be considered secure because there  
4                   is a company which is actually taking care of  
5                   the security of your private key and making sure  
6                   through their own network security that no one  
7                   actually has access to your private keys. It  
8                   also allows, in the event that you cannot  
9                   forget -- you cannot remember your access codes  
10                   or passwords or something like that, there's  
11                   some sort of way to get back whatever is in your  
12                   account. There's some sort of customer service  
13                   that can provide some sort of assistance if you  
14                   do lose your wallet or if you do lose your  
15                   log-in information.

16                   Whereas with mobile wallets or desktop  
17                   wallets, if your device becomes somehow  
18                   corrupted, if you lose your device or if you're  
19                   a victim of some sort of malware which actually  
20                   steals your information, your keys, and you lose  
21                   your wallet, well, then you lose your bitcoins.  
22                   There's actually no resource or little recourse  
23                   in order to get back whatever bitcoins you may  
24                   have lost. So there are some advantages and  
25                   disadvantages to each wallet.

1                   If we move on to hardware wallet, which --  
2                   I suppose it's the second picture from the  
3                   right. This is similar to a USB key, but it's a  
4                   device that's created simply and specifically  
5                   for the storage of your private keys and your  
6                   wallet, meaning that it -- this small encrypted  
7                   device can keep the -- well, the ability to  
8                   spend associated bitcoins completely free from  
9                   the internet and even when connected to a  
10                  computer, it never release the private keys to  
11                  the computer itself. It simply allows the  
12                  access to the wallet to actually conduct  
13                  whatever transaction that would be conducted  
14                  online.

15                  And finally at the end, completely on the  
16                  right we see a paper wallet. Now, a paper  
17                  wallet is essentially just that. We can see a  
18                  public key and we can see a private key. And in  
19                  order to spend these funds you would either need  
20                  to -- well, you would need to take a picture or  
21                  use the actual funds themselves, use the actual  
22                  piece of paper itself, to rebuild the wallet to  
23                  be able to send the funds that are associated  
24                  with it.

25                  These are both considered cold storage,

1                   which means that if done -- if prepared  
2                   properly, then -- particularly on the paper  
3                   wallet, then these private keys have never been  
4                   online. So, now, the -- if you are preparing it  
5                   properly, like I said, for a paper wallet, you  
6                   should be preparing this on a computer that is  
7                   disconnected from the internet if you're going  
8                   to be doing that. So in order to spend funds  
9                   that are associated to either the paper wallet  
10                  or the hardware wallet, it takes a little bit  
11                  more time and effort in order to do so. And  
12                  like I mentioned, that's why they are considered  
13                  cold wallets. Much enhanced in terms of  
14                  security versus the other wallets.

15                         The paper wallet can be an automatic -- so  
16                         a visit to an ATM machine. If you do not have  
17                         an existing account and you do deposit funds,  
18                         then you will be simply granted -- or in  
19                         exchange you will receive a paper wallet. So  
20                         it's as simple as that to obtain a paper wallet.  
21                         And as far as hardware wallets go, they tend to  
22                         be less popular due to -- well, I guess people  
23                         being unsure about dealing with them as well as  
24                         they tend to be an investment of more than \$100  
25                         or so right off the bat, so for the casual user

1                   they tend not be to be so popular.

2           Q       That makes sense.  Let's turn to the next slide  
3                   which has to do with seed phrase.

4           A       (AG) Yes.

5           Q       And explaining what that concept is.  And just  
6                   to alert you to this as I look at the clock, I  
7                   want to make sure we track along and I leave  
8                   sufficient time for other counsel to ask some  
9                   questions.  So if you spot a shortcut, you can  
10                  take it.  And if I have other questions, I'll  
11                  slow you down to ask them as I appreciate -- not  
12                  blaming anyone for going slowly because I asked  
13                  a whole bunch of questions already.

14                         But why don't we turn to slide 14, please,  
15                         and help us understand what the "seed phrase"  
16                         refers to.

17          A       (AG) Sure.  Absolutely.  So the seed phrase  
18                   would be kind of your backup to your wallet.  So  
19                   depending on the type of wallet you have, it  
20                   will be 12 to 24 words.  Now, just having these  
21                   words and knowing the type, or in some cases not  
22                   even the type but typically the software used to  
23                   create the wallet in the first place, you can  
24                   recreate whatever wallet has been lost.

25                         So in the event that you do lose or -- your

1 device but you do have these words written down  
2 somewhere, then you can recreate and rebuild  
3 your wallet and regain access to the funds.  
4 Now, this is important for law enforcement in  
5 the event that we find something like this,  
6 rather than actually being able to access  
7 whatever device had bitcoins stored on them.

8 So if we can go to the next slide, please.

9 (AV) Okay. Now we're going to go through  
10 the different types of methods available to  
11 citizens to be able to purchase cryptocurrency.  
12 So the most popular out there is a public  
13 exchange otherwise known as a centralized  
14 exchange. This is a third party that  
15 facilitates the purchase, sale and conversion of  
16 cryptocurrency from one to another. They  
17 usually are funded through the transaction fees  
18 that they charge their customers. In order to  
19 create an account with one of these entities,  
20 normally they'll accept all sorts of payment,  
21 whether it be bank transfers, credit card, money  
22 orders, gift cards. You can even send a  
23 transfer through Canada Post. And then often  
24 times they will use the service of a third-party  
25 service provider in order to be able to accept

1                   this payment. And the reason that they have to  
2                   do that, at least here in Canada, is just an  
3                   unwillingness by the Canadian banks to support  
4                   cryptocurrency purchases. So the exchanges have  
5                   to use this third-party service provider as the  
6                   banks will not facilitate a bank transfer to go  
7                   directly to that exchange.

8                   The reason that I bring this up is, at  
9                   least from a law enforcement perspective, this  
10                  does tend to further distance the funds from the  
11                  source which, you know, potentially can help  
12                  facilitate money laundering if such -- you know,  
13                  a target is pursuing that.

14                  Now, upon receiving the funds a client is  
15                  usually asked to provide some KYC. So the --

16                  Q    I'll pause to make sure we have it. KYC, know  
17                  your customer?

18                  A    (AV) Sorry. Yeah.

19                  Q    No, that's okay. Carry on.

20                  A    (AV) Yeah, know your customer. And so the  
21                  exchange will usually ask for -- usually a  
22                  picture of the person requesting the account  
23                  holding their driver's licence or some sort of  
24                  picture ID next to them, and then they will send  
25                  this image forward to the exchange who will run

1 a computer algorithm against it and confirm that  
2 the person holding the driver's licence is  
3 actually the same person that's in that ID. And  
4 when they're quite convinced that you are in  
5 fact who you say you are, they'll follow up with  
6 some sort of request for proof of address, a  
7 utility bill or whatnot.

8 Now, as we know, legislation has just come  
9 into play here in Canada that says these  
10 exchanges now must be registered as money  
11 service business and that they need to collect  
12 KYC, but this is a process that they've been  
13 doing for a long time, often maybe as the role  
14 as foreign money service businesses in dealing  
15 with -- in the oversight of FinCEN perhaps in  
16 the States but also as a method to just protect  
17 themselves from frauds.

18 There's been hacks that have happened in  
19 the past where customer information has been  
20 captured and a lot of these images of an  
21 individual holding their driver's licence are  
22 available for sale on the darknet and are being  
23 used by corrupt entities trying to create  
24 accounts with the exchanges. So that's why they  
25 run this computer algorithm and ensure that the

1 client is confirmed.

2 Q If I could just pause to make sure we've got the  
3 reference. You referred to some recent  
4 legislation. Is that -- is it the case that  
5 you're referring to amendments that took effect  
6 at the start of June of this year to the  
7 Proceeds of Crime (Money Laundering) and  
8 Terrorist Finance Act? Is that accurate?

9 A (AV) That is correct.

10 Q All right. Carry on.

11 A (AV) So once a client is able to create an  
12 account, once they've gone through all of this  
13 process, they're able to create an account on an  
14 exchange and they're able to transact on there,  
15 either purchase cryptocurrency, sell  
16 cryptocurrency or convert one type for another,  
17 say, as a conversion from bitcoin over to  
18 litecoin, which is different cryptocurrency.

19 The exchange will usually hold what's  
20 called a custodial wallet, whereas they'll hold  
21 the customer's private keys and take custody of  
22 those. So the customer themselves is no longer  
23 really in control of this; however, any time a  
24 transaction occurs with their funds their  
25 account shows up as either debited or credited.



1                    Now, all the cryptocurrency private keys  
2                    aren't actually retained within the exchange  
3                    themselves and that's to protect both themselves  
4                    and the clients from potential hacks. So they  
5                    actually store the majority of their reserves in  
6                    a cold wallet offline and they'll only keep  
7                    what's necessary in order to be able to handle  
8                    transactions to meet the supply and demand of  
9                    those transactions within their hot wallets.  
10                   And then as the reserves deplete, they can  
11                   replenish them from their cold wallets offline.  
12                   So typically that's how these exchanges work.

13                   Now, an example of one of these exchanges  
14                   that I'd like to bring up is Quadriga, which  
15                   is -- you know, had a -- basically rose to fame  
16                   in January of last year when it was reported  
17                   that their CEO, 30-year-old Gerald Cotten, died  
18                   while in India, honeymooning with his wife. And  
19                   media reports quickly came out after that, you  
20                   know, Gerald Cotten was the only person in  
21                   possession of the private keys accessing these  
22                   cold wallets offline that held up to  
23                   \$250 million in the -- in clients'  
24                   cryptocurrency assets.

25                   So, you know, of course the international

1 community was completely shaken.  
2 76,000 customers had lost potential access to  
3 their cryptocurrency assets. Now, Quadriga  
4 wasn't able to actually meet the demands of  
5 everybody trying to withdraw their assets at  
6 this time, so they had to declare bankruptcy and  
7 were put under the trustee of Ernst & Young.  
8 Simultaneously the RCMP began an investigation  
9 into this out of Milton, Ontario, just based on  
10 suspicious nature of Gerald Cotten's death and  
11 the activities that ensued.

12 So that's an ongoing investigation and I  
13 won't speak to that, but what I did want to  
14 highlight is just some of the findings that have  
15 been published by the Ontario Securities  
16 Commission and Ernst & Young and which are  
17 actually available in the overview report. And  
18 that's just, you know, how something like this  
19 could have potentially happened, and I think  
20 from -- the findings of Ontario Security  
21 Commission and Ernst & Young shows that in fact  
22 the private keys accessing those cold -- the  
23 funds in the cold storage are not really at  
24 issue here because those cold storages are --  
25 were relatively close to being empty. But what

1                   in fact happened was that the CEO, Gerald  
2                   Cotten, was manipulating the assets that were in  
3                   there. He was creating fictitious individuals  
4                   and transferring assets using real customers'  
5                   cryptocurrency that was there. He was paying  
6                   new customers with -- or sorry, old customers  
7                   with new customers' funds, basically carrying  
8                   out a Ponzi-type scheme. And it just goes to  
9                   show how could something like this potentially  
10                  happen without -- we certainly certainly need more  
11                  oversight and regulatory monitoring of what  
12                  happens within a public exchange.

13                         Now, we've talked already at length about  
14                         how all these transactions that occur on the  
15                         blockchain are visible to everybody. Well, one  
16                         thing we didn't mention is the exception to that  
17                         or one of the exceptions is when a transaction  
18                         goes into an exchange. And so all of the  
19                         dealings that happen within are off of that  
20                         blockchain and are only visible to that exchange  
21                         themselves, and unless they actually have  
22                         accountability for the transactions that they're  
23                         doing that -- doing within there, then this type  
24                         of thing can happen.

25                                 It also begs the question that -- you know,

1                   the idea that one person could be the sole  
2                   entity in control of private keys accessing up  
3                   to \$250 million in customers' assets, you know,  
4                   at one point in time this was inconceivable.  
5                   And, now, yes, this may not have been what  
6                   happened in this case, but it shows that the  
7                   potential threat is there and there needs to be  
8                   more oversight over the cold storage wallets  
9                   that are held within these exchanges.

10                   Now, currently the exchanges don't publish  
11                   the amounts that are in their cold storage  
12                   wallets, so nobody had any indication that  
13                   Quadriga didn't have the balance in there  
14                   necessary to support the degree of operations  
15                   that they were controlling there. So more  
16                   transparency in regards to that I think would be  
17                   very helpful moving forward.

18                   Q   Quadriga was a notorious case and of course a  
19                   Vancouver-based case that was actually written  
20                   up in the media, including Vanity Fair. It  
21                   achieved a certain prominence. But when you  
22                   describe the exchanges, it's sort of a point --  
23                   from the point of view of tracing that the  
24                   exchange itself can be the dead end that breaks  
25                   what might otherwise be a chain or a trail that

1                   could be followed by investigators?

2           A       (AV) Absolutely. We can see, using these  
3                   aftermarket software tools, when a transaction  
4                   has entered the exchange. We cannot see what  
5                   happens within than exchange, nor can we see  
6                   what happens when it -- if a transaction leaves  
7                   that exchange. So that's why we -- you know,  
8                   we'll need to go forward and get production  
9                   orders under lawful authority to be able to get  
10                  some information in regards to that. Now --

11          Q       Thank you. I was going to direct you to the  
12                   next slide, which talks about KYC protocols with  
13                   public exchangers.

14          A       (AV) Yes. So as I had mentioned before, when  
15                   trying to gain an account with one of these  
16                   exchanges -- and they are not all the same.  
17                   They all have their own different KYC protocols  
18                   especially here in Canada. Now, this is  
19                   probably going to become a little bit more  
20                   standardized since regulations have been put  
21                   into play, but a lot of the more reputable ones,  
22                   as I said, will ask for driver's licence ID and  
23                   that sort of information. So this is the kind  
24                   of information that we can capture if we have  
25                   the lawful authority to go forward with a

1 production order, and certainly some of it  
2 depends on how the individual purchased their  
3 cryptocurrency. So as you can see on the slide,  
4 bank account information and credit card  
5 information. Obviously that will be reliant on  
6 the method of payment used.

7 Next slide, please.

8 Q We turn here to public -- sorry, from public  
9 exchangers to private exchangers.

10 A (AV) Right. So private exchangers are -- it's  
11 basically a peer-to-peer platform which connects  
12 buyers and sellers and they post their fees, so  
13 the exchange doesn't necessarily control the  
14 fees; the individuals do themselves. And then  
15 they connect with who they want to purchase  
16 from. So it's almost similar to what you would  
17 see on Kijiji or Craigslist where if you're a  
18 seller of cryptocurrency or you want to purchase  
19 it, you would put your ad up there and somebody  
20 would, you know, contact you if they're willing  
21 to pay the fees that you're offering.

22 So from a law enforcement perspective this  
23 is a very risky way to be able to go and  
24 purchase your cryptocurrency. For one, it's  
25 extremely expensive in comparison to what the

1 exchanges charge, which is traditionally about a  
2 quarter of a percentage of up 4 percent. Now,  
3 that may be increasing with the increase in the  
4 price of bitcoin right now. I'm not sure. But  
5 with private exchangers you can pay anywhere  
6 from 10 to 15 percent. And most of the time the  
7 reason that you're paying these fees it because  
8 it offers that anonymity that you do not get  
9 when you're dealing with the exchanges.

10 Now, some of these platforms will take  
11 payment in, you know, credit card or bank  
12 transfer, so KYC may actually be conducted, but  
13 a lot of the time cash transactions is the way  
14 to go and these individuals or these exchangers  
15 will meet the buyer in a Tim Hortons or in some  
16 dark alleyway to conduct the transaction.

17 Now, as we had said, it takes at minimum of  
18 ten minutes but can take up to an hour or more  
19 for that transaction to be authenticated and to  
20 appear on the blockchain. And normally we would  
21 want to wait three or four validations before  
22 that happens, so before you can be actually  
23 convinced that your transaction has gone through  
24 could take 30 minutes to 60 minutes. So if  
25 you're meeting some stranger for an agreed upon

1 price to be able to transact cash for bitcoin,  
2 what are the chances that that individual is  
3 going to, like, stand there and wait those  
4 30 minutes to 60 minutes to confirm that the  
5 transaction has gone through? It's highly  
6 likely, which -- unlikely, sorry, which puts the  
7 individual at risk of fraud. There's also been  
8 cases where individuals have been assaulted and  
9 their bags of cash just stolen as the  
10 individuals have run away.

11 There are several exchanges out there.  
12 Paxful is one of the more common ones, and they  
13 actually boast over 300 payment methods, which  
14 includes cash and various gift card  
15 transactions. So it makes it very difficult  
16 from a law enforcement perspective to be able to  
17 follow the flow of funds or collect KYC when  
18 needed.

19 Next slide, please.

20 Q And we move now to the topic of bitcoin ATMs.

21 A (AV) Right. So bitcoin ATM machines. So these  
22 are just another mode of exchange. These  
23 machines are available all over Canada.  
24 Currently we just -- have as of yesterday just  
25 under 1,000 of these machines across the country



1                   and they basically allow anybody to go in and  
2                   purchase bitcoin or other types of  
3                   cryptocurrency using cash. They offer -- they  
4                   also offer higher exchange rates, you know, 10  
5                   to 15 percent. They can be used certainly as a  
6                   facilitator for money laundering but they also  
7                   provide an ability, from my opinion, for  
8                   somebody who's interested in cryptocurrency to  
9                   be able to just go to a machine and input \$20  
10                  and see how it works. Now, some of these  
11                  machines will allow you to -- or sorry, they  
12                  will all allow you to purchase cryptocurrency,  
13                  and then some of them will allow you to sell  
14                  cryptocurrency as well.

15                  Now, there's different ways to be able to  
16                  run one of these machines, to be an operator of  
17                  it, and that is to either purchase one of these  
18                  machines and have an open -- or sorry, have an  
19                  open account with an exchange. And so every  
20                  time a purchase is made at this ATM machine it  
21                  will mirror the transaction with your open  
22                  account at the exchange. That makes sure that  
23                  the wallet used to support the bitcoin ATM  
24                  machine is fully replenished and will always  
25                  meet the supply and demand of that particular

1 machine. It also ensures that the operator of  
2 that machine is paying the same amount for the  
3 cryptocurrency as it's being sold for. And that  
4 just helps deal with some of the volatility  
5 issue. So if the operator isn't able to get to  
6 their machine or fill up their own  
7 cryptocurrency wallet, their relationship with  
8 the larger exchange will just help facilitate  
9 that and run the process through.

10 The other option is to purchase one of  
11 these machines and support it using your own hot  
12 wallet. Now, as you can imagine, you would have  
13 to have a lot of reserves to be able to keep in  
14 this hot wallet and be able to run it. Now,  
15 there's a couple of instances that I can  
16 highlight in which individuals have used this  
17 machine in order to be able to -- these machines  
18 in order to be able to facilitate money  
19 laundering schemes.

20 So in May of 2019 in Spain a criminal  
21 organization was getting drugs from the  
22 Colombian cartel, importing the drugs, selling  
23 it in Spain and then they needed something to do  
24 with this -- with the cash that they were  
25 bringing in from the sale. So they ended up

1 with two of these bitcoin ATM machines and they  
2 fabricated a money service business. They were  
3 feeding the cash into these machines and then  
4 instantly transacting the cryptocurrency over to  
5 Colombia, who were able to get the proceeds of  
6 these sales without actually ever having to  
7 touch the elicited cash and were able to settle  
8 debts almost immediately.

9 These individuals in Spain had created this  
10 fictitious money service businesses, fabricated  
11 all their books and then you were able to  
12 justify their money service business, their  
13 shell company essentially, as justification for  
14 this influx of cash.

15 Spain -- the Spanish police became aware of  
16 this and they took them down in May of last  
17 year. And then just in July of this year a  
18 California man pled guilty for basically doing  
19 the same thing. He exchanged up to \$25 million  
20 in cash through 17 ATM machines that he had had  
21 disbursed across California which he did with --  
22 provided individuals the addresses so they could  
23 go and use these machines as well as he  
24 facilitated in-person transactions. And he did  
25 the same thing, he created a fictitious money

1 service business to justify the proceeds of this  
2 sale. Now --

3 Q Are there any -- I'm sorry. Are there any KYC  
4 or any sort of mechanisms that prevent, if I'm  
5 drug dealer, me from simply taking the  
6 machine -- I don't know if they even speak to  
7 this issue of setting up the machine in my own  
8 garage to feed in stacks of 20s generated from  
9 drug dealing and then converting that out to  
10 bitcoin and hiding the trail if I move it around  
11 from there?

12 A (AV) Well, as a third-party operator -- service  
13 operator of these machines, now, you know,  
14 regulations require reporting and anything over  
15 \$1,000 -- which I believe doesn't take effect  
16 until next year, although the majority of the  
17 operators are now facilitating it, is anything  
18 over \$1,000 requires KYC. But these are the  
19 more reputable operators out there that are  
20 trying to be compliant and abide. As well as if  
21 they don't flag this and report to FINTRAC, then  
22 if they have an account already set up with the  
23 exchange to mirror the transactions, then that  
24 exchange is likely going to be able to capture  
25 that information through reporting.

1                   But in your example, to have a criminal  
2                   organization purchase one of these machines and  
3                   run them in their garage, then no, there would  
4                   likely be no reporting take place. And if  
5                   there's no mirroring with an exchange, there  
6                   would be no safety net to capture that  
7                   information. And unless law enforcement was  
8                   particularly looking at them and watching the  
9                   blockchain transactions and investigating it, it  
10                  would likely go unnoticed.

11                  So with bitcoin ATM machines, their use has  
12                  increased substantially. In the last year there  
13                  has been a hundred percent increase in these ATM  
14                  machines. So where there was about 6,000 of  
15                  them worldwide last November, we now see over  
16                  12,000 of them out there potentially because  
17                  they offer an ability for people that  
18                  traditionally have been unbanked to be able to  
19                  now deal and to transact, move currency anywhere  
20                  across the world in a matter of minutes,  
21                  providing somebody has access to one of these  
22                  machines in one of the 74 countries out there.  
23                  But it also is a very -- a tool susceptible to  
24                  laundering as we have mentioned. So there's  
25                  been a lot --

1           Q     In a sense there you sort of capture the good  
2                   and the bad, don't you? That on the one hand  
3                   there's a sort of -- and I think that's been  
4                   sort of the more optimistic discussion around  
5                   bitcoin in particular is that this may provide a  
6                   mechanism for what you call the unbanked people  
7                   who don't have access to regular bank accounts,  
8                   especially in the developing world, to suddenly  
9                   have an easy means of transacting and moving  
10                  money around, et cetera, on the other hand a  
11                  vulnerability to crime and money laundering?

12           A     (AV) Absolutely. And these new KYC  
13                  requirements, it's very obvious to see that  
14                  they're being implemented. But I know from law  
15                  enforcement out in British Columbia who had been  
16                  dealing with one of the operators out there, he  
17                  had set a very minimal KYC requirement in his  
18                  machine in his effort to try to deter money  
19                  laundering through them and during that time  
20                  since, he had implemented this low KYC he'd  
21                  noticed that his business had dropped by  
22                  30 percent.

23                         So there's not much incentive on the  
24                         operators to be able to try to keep those  
25                         requirements for KYC low and do their part to be

1                   able to support this. At least beyond what has  
2                   been required by FINTRAC and the Proceeds of  
3                   Crime (Money Laundering) and Terrorist Financing  
4                   Act.

5           Q       What sort of KYC measures can the ATM operator  
6                   take? I take it they could use a picture --  
7                   take a picture of whoever is there at the  
8                   machine feeding in the bills?

9           A       (AV) Yeah. So they can -- it's really up to  
10                   them what sort of, you know, KYC they want to  
11                   implement. They can take a picture, ask for  
12                   photo identification. They can ask for SMS  
13                   verification, which is a cellphone number. But  
14                   in this day and age anybody can download an app  
15                   to change the number of their cellphone  
16                   temporarily or use a burner phone.

17           Q       Yeah.

18           A       (AV) There's also the ability to put a  
19                   fingerprint -- to capture a fingerprint in order  
20                   to be able to utilize those machines. But here  
21                   in Canada where our right to privacy is  
22                   inherent, you know, it's not something I think  
23                   most people would feel very comfortable in  
24                   doing.

25                                   Now, most of these machines will capture an

1 image of the user as they approach the machine  
2 to utilize it, but, you know, there's no  
3 mechanism in place to ensure that that's been  
4 captured until they reach the threshold over the  
5 \$1,000 mark. So it's very easy for anybody to  
6 just do a quick camera dodge or put their thumb  
7 over the camera to make sure --

8 Q Or wear a mask these days.

9 A (AV) Yes. Yeah. Well, exactly; right? Next  
10 slide.

11 Q Why don't we -- maybe we can go quickly through  
12 the next few. I think they describe --

13 A (AV) Sure.

14 Q Number 17 there we see -- and I'll let you do  
15 that. Thank you.

16 A (AV) Yeah. So I'll run through quick. We do  
17 have a site available to us on coinATMradar.com  
18 where anybody who wants to publish their machine  
19 in order to gain customers can post it on this  
20 website, so it's available to the entire world.  
21 We pulled this stat up here from Alberta. So  
22 you can see there a map that shows there are  
23 101 ATMs currently in the Vancouver area.

24 Next slide, please. And then what you can  
25 do is go in there and put in your postal code



1                   and it will pull up a list of all of the ATMs  
2                   within the area and starting from that -- within  
3                   the closest vicinity to you and just getting  
4                   further and further and further away.

5                   So I put in the address for the Cullen  
6                   Commission, and this is the first machine within  
7                   the vicinity. And so as we can see on this  
8                   page on the left-hand corner, the operator is  
9                   Bitcoiniacs and there's some contact information  
10                  there for Bitcoiniacs. Down below you'll see  
11                  the location, which is Waves Coffee House at 900  
12                  Howe Street, as well as the operating hours of  
13                  the actual coffee shop.

14                  On the right-hand side you'll see the  
15                  bitcoin machine details. This particular  
16                  machine will allow an individual to both  
17                  purchase and sell bitcoin as well as litecoin,  
18                  and then it will have the fee there that the  
19                  operator charges.

20                  And then in the red highlighted box you'll  
21                  see "limits and verification." So this  
22                  particular operator, Bitcoiniacs, is very, very  
23                  compliant and is doing their role to try to  
24                  prevent money laundering, which is -- you know,  
25                  here they're requesting SMS verification for any

1 purchase between \$20 and \$200. And anything  
2 over \$201 they actually are requesting ID scan  
3 verification. So this is quite rare when it  
4 comes to bitcoin ATMs. The majority of them  
5 will not be asking for any kind of verification  
6 under \$1,000.

7 And then in the bottom, just a nice to  
8 know. This is actually the world's first  
9 bitcoin machine ever in Vancouver at this  
10 location, which is quite interesting. And as  
11 you can see, when it was opened there in 2013  
12 the value of bitcoin was at \$211 per bitcoin,  
13 and just a day or two or so ago it was at  
14 23,000. I imagine it's increased more since  
15 then.

16 Next slide, please.

17 (AG) This is simply a slide indicating that  
18 police are aware of the use of these bitcoin ATM  
19 machines in British Columbia and surrounding  
20 areas. Next slide, please.

21 (AV) Okay. Another mode of exchange are  
22 these prepaid bitcoin debit cards. So there are  
23 several merchants out there now that are  
24 accepting bitcoin as a form of payment or other  
25 cryptocurrencies, but they're still very few and

1 far between. And the reason really is based on  
2 the volatility of specifically bitcoin in which  
3 a merchant can't be sure of the purchasing  
4 power. So if they accept \$20 for a cup of  
5 coffee, then perhaps the next day that \$20 will  
6 only be a value of \$10. So it really doesn't  
7 make sense for them necessarily to accept it at  
8 this point.

9 So these prepaid bitcoin debit cards offer  
10 an alternative for that. So somebody -- anybody  
11 can order one these cards and transfer  
12 cryptocurrency over to a third-party operator  
13 who will then fund these cards with currency  
14 that the person can now spend where -- anywhere  
15 that accepts Visa or Mastercard. So they're  
16 fairly easy to get. You can just go online and  
17 you can order one of these plastic or virtual  
18 cards. They're extremely vulnerable to money  
19 laundering because when we are purchasing online  
20 we can use fake ID, we can use straw buyers who  
21 can get a whole bunch of these cards and then  
22 transfer the PIN number and even just the  
23 virtual card number over to the bad actor. They  
24 ask for very little KYC, if you go onto a lot of  
25 these sites. They ask for your first name,

1 phone number and an email. If you want an  
2 actual plastic version of the card instead of a  
3 virtual one, they'll ask for a PO box.

4 And then of course there's the idea of the  
5 gift cards. So gift cards, they want an email  
6 and a name, PO box if you want a plastic card.  
7 They are -- because gift cards are considered  
8 closed loop, they won't actually fall under the  
9 KYC regulations and neither the prepaid cards  
10 nor the gift cards are considered monetary  
11 instruments, which means, you know, anybody can,  
12 like, cross any border with any amount of these  
13 cards and not be responsible to account for  
14 those. Next slide, please.

15 Now, a couple more unofficial modes are  
16 over-the-counter brokers. So when the -- when  
17 an -- or a transaction goes through an exchange,  
18 an exchange is technically required to keep,  
19 like, a public order book where they mark all  
20 the transactions that go through their exchange.  
21 So if there is a very large amount of  
22 cryptocurrency being purchased or sold, it has  
23 the potential to rock the market. And people --  
24 the cryptocurrency community would get kind of  
25 bent out of shape, what is happening; what does

1                   this individual know that we don't know; sell,  
2                   sell, sell, or whatnot. So these  
3                   over-the-counter brokers provide an opportunity  
4                   for whales to exchange very large amounts of  
5                   cryptocurrency outside of an open exchange. So  
6                   they're normally run by an exchange but not  
7                   under the same type of scrutiny. And personally  
8                   I'm not going to speak much to them because I'm  
9                   not an expert in this area, but I know that they  
10                  are quoted by Chainalysis as being very  
11                  susceptible to money laundering because they  
12                  have don't have the same oversight.

13                  And then there's private offchain  
14                  transactions. Now, I've said before the  
15                  exchange -- what happens when a transaction goes  
16                  through an exchange is offline; it's not  
17                  captured on the blockchain. Well, the same can  
18                  be -- can ring true with these private off-chain  
19                  transactions. Now, how this can occur is if I  
20                  were to conduct a transaction with one  
21                  individual and I were to send my friends from my  
22                  bitcoin address to their bitcoin address, it  
23                  would be captured onto the blockchain. However,  
24                  as we know, the individual that has access to  
25                  that private key can access the cryptocurrency.

1                   So if I were to just provide the private key to  
2                   another individual, I've essentially transferred  
3                   the funds over to that person without it being  
4                   captured at all on the blockchain. The same is  
5                   true if I had a paper wallet and I wanted to  
6                   capture an image of it and giving it to them.  
7                   So basically I'm giving them access and control  
8                   of the cryptocurrency without actually  
9                   documenting it on the blockchain.

10                   Now, there's something else called the  
11                   lightning network, which will -- is basically  
12                   like running a tab. It's -- in order to help  
13                   deal with some of the scalability that happens  
14                   with bitcoin on the blockchain, and that is the  
15                   length of time that it takes to process  
16                   transactions. So the lightning network will  
17                   enable somebody to transact with another entity,  
18                   but then all of the individual transactions that  
19                   occur between them will not be captured until  
20                   the account is settled. So as I said, running a  
21                   tab, say, with a bar over a period of a couple  
22                   weeks and you may attend to this particular  
23                   location 5, 10, 15 times and have very -- like,  
24                   transactions occur, but only once that tab is  
25                   settled will it appear on the blockchain as one

1                   single transaction for the total amount that --  
2                   what has occurred.

3                   So it helps deal with the scalability but  
4                   from a law enforcement perspective it is quite  
5                   difficult because we're unable to see what has  
6                   occurred throughout those various transactions  
7                   or even to know if there's been more than one.

8                   Next slide, please.

9                   MR. MARTLAND: I wonder, Mr. Commissioner, if I might  
10                   suggest -- this may be a useful time to suggest  
11                   a break, maybe for 10 minutes.

12                   THE COMMISSIONER: Very well. We'll take 10 minutes,  
13                   Mr. Martland. Thank you.

14                   MR. MARTLAND: Thank you.

15                   THE REGISTRAR: This hearing is adjourned for a  
16                   10-minute recess until 11:26 a.m. Please mute  
17                   your mic and turn off your video. Thank you.

18                   **(WITNESSES STOOD DOWN)**

19                   **(PROCEEDINGS ADJOURNED AT 11:17 A.M.)**

20                   **(PROCEEDINGS RECONVENED AT 11:26 A.M.)**

21                   **AARON GILKES, a witness**  
22                   **for the commission,**  
23                   **recalled.**

24                   **ADRIENNE VICKERY, a**  
25                   **witness for the**





1                   June 1st, 2020. So this year. They will also  
2                   all have to report on any suspicious  
3                   transactions. And they have to improve their  
4                   ability to be prepared to report on large cash  
5                   transactions as -- I believe also foreign money  
6                   service businesses fall into this category,  
7                   providing they provide services to Canadians.  
8                   So they don't necessarily have to be located in  
9                   Canada, but if they offer services to Canadians  
10                  citizens, then they will.

11                 Q    And so that's a change from a requirement that  
12                   used to be that if the MSB had, let's say,  
13                   incorporated in Canada, office in Canada, agents  
14                   in Canada, they were under that regime, but  
15                   that's been changed to actually cover off  
16                   situations where the MSB isn't incorporated  
17                   here, may not have an office here or agents here  
18                   and yet if it's conducting business here, it  
19                   falls under that regime; is that your  
20                   understanding?

21                 A    (AV) I'm not sure how foreign money service  
22                   businesses were dealt with prior to this  
23                   legislation.

24                 Q    All right. Why don't I let you carry on, then,  
25                   with slide 24.

1           A     (AV) Okay. So bitcoin is number 1. We keep  
2                    talking about all these different  
3                    cryptocurrencies. In fact there's over 7,700 of  
4                    them that exist. But over 62 percent of all  
5                    transactions with cryptocurrency is dealt with  
6                    bitcoin. So it is by far number 1, but it does  
7                    have its flaws.

8                                 First and foremost is the lack of privacy.  
9                    As we've already talked about, the type of  
10                   information that's available and transparent on  
11                   the blockchain poses a problem, yes, to the  
12                   criminal element, but it also poses a problem to  
13                   the regular public. Just like I wouldn't want  
14                   to put my bank account information up here on  
15                   the screen for everybody to see the amount that  
16                   currently is in or not in my bank account, I  
17                   don't necessarily want everybody to be able to  
18                   see my transactions within my address on the  
19                   blockchain either.

20                                 There's also potential for high transaction  
21                   fees. During times of high demand you must pay  
22                   a high transaction fee in order to entice the  
23                   miners as we talked about before. Now, this can  
24                   vary. At times it's worth about 40 cents per  
25                   transaction fee up until -- just the other day

1                   we're now at \$11 per transaction fee. Back on  
2                   December 17th of 2017 where bitcoin was at its  
3                   highest, there was actually times where the  
4                   average transaction fee was about \$55 US, which  
5                   is -- it's not conceivable to think that people  
6                   would be paying that kind of transaction fees  
7                   for simple purchases.

8                   And then obviously the high volatility.  
9                   You can't be sure of the purchasing power of it,  
10                  so, you know, it's hard to use for regular  
11                  transactions. The long wait times. And Acting  
12                  Sergeant Gilkes already talked about this, how,  
13                  you know, bitcoin can only transact about seven  
14                  transactions per second compared to Visa, which  
15                  can do 24,000 per second.

16                  It's also not backed by a central  
17                  authority, which means if your account's been  
18                  compromised, there's actually nobody that you're  
19                  able -- there's no legal discourse available for  
20                  you to be able to fall back on and get  
21                  reimbursed for transactions that have been lost  
22                  or stolen.

23                  And transactions are irreversible. So as  
24                  you saw, that public address that exists, which  
25                  is what we provide individuals in order to be

1                   able to send us funds, is a really long  
2                   alphanumeric code. And if you inadvertently put  
3                   in the wrong upper case where it's supposed to  
4                   be a lower case or you just put in the wrong  
5                   address, then you've essentially sent those  
6                   funds off to cyberspace or to somebody else's  
7                   address and there's no mechanism in place to be  
8                   able to recover that.

9                   Next slide, please.

10                  Q    You speak here about other -- the alt coins,  
11                   stable coins, privacy coins, et cetera?

12                  A    (AV) Yeah. So this is kind of the  
13                   cryptocurrency community's response to some of  
14                   these deficiencies that exist within bitcoin.  
15                   The stable coins deal with the issue of  
16                   volatility in that they're backed by some sort  
17                   of fiat currency or stable commodity as we had  
18                   talked about at the beginning. And this  
19                   commodity will usually hold as -- act as  
20                   collateral, and so the entity who's managing it  
21                   will keep the equivalent of the amount that  
22                   they've lent out in actual assets. So it will  
23                   always be a balance and that's where the change  
24                   doesn't -- the change in volatility isn't really  
25                   seen. Tether is one of the coins currently that

1 is a stable coin and one of the top  
2 cryptocurrencies out there.

3 Privacy coins. So these help deal with  
4 some of the privacy issues that we see with  
5 bitcoin. Yes, you know, with bitcoin we can't  
6 see who the holder of that account is, but we  
7 can see what addresses it was sent by, to whom  
8 it was received, where some of these privacy  
9 coins will circumvent that and offer embedded  
10 encryptions within the transactions. So that  
11 information is not actually capable of being  
12 captured, not even with these aftermarket  
13 software tools that will usually provide  
14 attribution for some of the other coins out  
15 there.

16 And then there's alternative coins. So  
17 alternative coins truly refers to any other coin  
18 other than bitcoin. But there's many options  
19 out there that will provide their platform, such  
20 as the Ethereum blockchain, to be able to  
21 support smart contracts. So, for instance,  
22 we've talked about the blockchain and the  
23 transparency that exists there and the ability  
24 to kind of follow the flow of funds, and you can  
25 do that with all sorts of information.

1                   So Walmart has adopted the IBM food trust  
2                   blockchain in which they're able to be able to  
3                   follow the flow of all their crops -- or their  
4                   produce, sorry, from crops through distribution  
5                   centre to store shelf, and they mandate any  
6                   supplier dealing with produce in their  
7                   businesses to be able to put this information on  
8                   the blockchain. So now if they have, say, a  
9                   head of lettuce that's linked to listeria, they  
10                  can look at the blockchain and see exactly which  
11                  distribution centres that head of lettuce flowed  
12                  through and which crop it originated from as  
13                  well as every other store shelf in Walmart --  
14                  businesses that may have some of these crops  
15                  that originated -- or produce that originated  
16                  from the same crops, and they can remove that  
17                  from their store shelf.

18                  So what used to take them seven days to be  
19                  able to trace this information, they can now do  
20                  so in a matter of two minutes and it's been  
21                  saving lives. It's worked so well for them that  
22                  they're actually moving this, you know,  
23                  blockchain ability over to their pharmaceuticals  
24                  as well.

25                  Next slide, please.



1                   ahead. Now, it doesn't mean that it's -- that  
2                   the project itself is dead. It is going to be  
3                   moving forward or it appears that it's going to  
4                   be moving forward but only once approval from  
5                   the US government has been provided. And it  
6                   will be becoming back as basically a backed --  
7                   or I will say a financially, well, backed system  
8                   in that it will be backed by whatever currency  
9                   of the market it's actually working in. So it's  
10                  actually not -- should not compromise the  
11                  stability of many smaller currencies which  
12                  happen to be out there.

13                         Now, it is based out of Switzerland, so  
14                         that does bring some questions in terms of  
15                         reporting, taxation, things like that, under  
16                         what categories would they fall and how  
17                         difficult would it be to obtain information --  
18                         as I mentioned before, for Canadian law  
19                         enforcement to obtain information on  
20                         transactions that would occur in Canada,  
21                         conducted by Canadians. But you would have to  
22                         reach overseas in order to obtain significant  
23                         information in relation to that.

24                                 Next slide, please.

25                   Q       This one's important to us. "Benefits and



1 Drawbacks of Cryptocurrency For Criminals &  
2 Money Launderers."

3 A (AV) So in this global economy cryptocurrency  
4 really does offer just a very quick, efficient,  
5 secure and affordable manner to be able to move  
6 value anywhere in the world in a matter  
7 of seconds. Providing somebody has access to  
8 the internet or to one of these 12,000-plus  
9 cryptocurrency ATM machines that exist in over  
10 74 countries, they can gain access to  
11 cryptocurrency. There's very minimal fees. I  
12 mean, yes, currently we're looking at about \$11  
13 average per fee, but that's -- or per  
14 transaction, but that's actually quite less.  
15 And it's accessible to people. So it doesn't  
16 matter if you're in an area that's traditionally  
17 unbanked, as I said, you can now be able to gain  
18 access to this crypto.

19 There's no limit on the amount of  
20 transactions that go through. As I had said  
21 before, you're not paying the fees on based on  
22 the amount of the transaction but how many  
23 parties are a part of that particular  
24 transaction. An added benefit is that  
25 conversion is not an issue. A bitcoin is a

1                   bitcoin is a bitcoin anywhere in the world, and  
2                   it can be compared to -- usually the US dollar  
3                   or the currency of that country.

4                   Global movement of value. So when dealing  
5                   with bulk cash, there's always the issue of  
6                   security, speed and cost. When moving large  
7                   amounts of bulk cash, a target is a susceptible  
8                   to interdiction by police, having other -- like  
9                   the couriers or other criminals stealing those  
10                  funds. The speed of time that it takes to move  
11                  bulk cash from, say, just even one point of this  
12                  country, from Vancouver through to Saint John's,  
13                  Newfoundland, can take a significant amount of  
14                  time let alone trying to move it across  
15                  international borders.

16                  And then the fee that's associated with  
17                  that because you're paying for couriers to move  
18                  your money, you're perhaps paying for officials  
19                  at the borders to be able to turn a blind eye.  
20                  There's significant cost involved in this, and  
21                  cryptocurrency avoids all of that. As I said,  
22                  almost instantaneously you can move money across  
23                  international borders, any amount, at most for  
24                  \$11 per transaction currently.

25                  It's pseudo anonymous, which is an

1                    advantage. It may be not as anonymous as what  
2                    we see with cash, but the ability to be able to  
3                    move that value so quickly circumvents that and  
4                    the information isn't available instantly to law  
5                    enforcement who the holder of that account is.  
6                    As well as with, you know, using fraudulent ID  
7                    and some of the aftermarket money laundering  
8                    tools that we'll talk about soon helps this.

9                                       There's also a strong lack of understanding  
10                    by law enforcement worldwide on what  
11                    cryptocurrencies are, how to investigate them,  
12                    the legal authorities to go after the seizure of  
13                    them and forfeiture of them as well as a lack of  
14                    global regulation. So we're very lucky here in  
15                    Canada that regulations are now in play, but in  
16                    this global economy there's nothing that  
17                    restricts a Canadian citizens from only  
18                    utilizing money service businesses within our  
19                    jurisdiction. So if you're a criminal and you  
20                    want to avoid these reportings by the compliance  
21                    entities, then you can easily just go online and  
22                    find yourself an exchange that doesn't have any  
23                    reporting requirements.

24                                       Now, some of the disadvantages are the  
25                    volatility of value. You know, we talked about

1                   that purchasing power and not being clear on  
2                   what that will be. So holding on to those funds  
3                   can certainly be a disadvantage if the value  
4                   were to drop exponentially.

5                   And then traceability. I think, you know,  
6                   there's -- most of these criminal entities will  
7                   read the newspapers, read media and they'll  
8                   see -- they're aware that law enforcement can  
9                   actually purchase some of these aftermarket  
10                  tools to be able to trace the flow of funds.

11                  And then just like there is a lack of  
12                  understanding by law enforcement, there's also a  
13                  lack of understanding by the criminal element on  
14                  what these cryptocurrencies are, how to use  
15                  them, which I think prevents a lot of them from  
16                  wanting to venture over and utilizing this,  
17                  specifically maybe some of the older portion of  
18                  the population.

19                  Next slide, please. Are you going to go?

20                  (AG) Oh, sure. Okay. So now we'll speak  
21                  in the next few slides about cryptocurrency and  
22                  criminality. So this is -- basically these are  
23                  the topics that we're going to be covering, so  
24                  basically various types of fraud, extortion,  
25                  Ponzi schemes, so forth and so on. Ransomware,

1 malware attacks, drug sales, human trafficking,  
2 terrorist financing and finally, while we're  
3 here, money laundering.

4 Next slide, please. So in order to  
5 explain, you know, cryptocurrencies and  
6 criminality, it's important to start at the  
7 beginning or as what I would consider the  
8 beginning of laundering funds via virtual  
9 assets. Now, what you're seeing on the screen  
10 is basically a screenshot of a webpage from -- I  
11 believe this is from 2002 or 2003. So as you  
12 can see from -- on the top right-hand of your  
13 screen that this is a site that was run by a  
14 team or a group of individuals, possibly a gang,  
15 called the Shadowcrew. Now, the Shadowcrew,  
16 what they were doing was laundering funds from  
17 stolen credit cards, identity theft, selling  
18 counterfeit identities, so forth and so on.  
19 Different types of frauds. And they were  
20 laundering these funds through a virtual asset  
21 or a virtual currency at the time called E-gold.  
22 Now, E-gold had been around since about 1996,  
23 and this particular bust of the Shadowcrew was  
24 2003, 2004. And there -- well, there was  
25 approximately 20 people who went to prison as

1 part of the Shadowcrew bust.

2 Now, E-gold itself was invited in 2007 and  
3 there were many bank accounts that were seized  
4 and assets were seized. And E-gold, it's  
5 important to mention, is that they were located  
6 in the United States at the time. So we'll kind  
7 of call that strike one for the virtual assets  
8 and money laundering. Next slide, please.

9 Then we can move on to a currency called  
10 Liberty Reserve, which is almost like a version  
11 2.0 of E-gold. So, now, we had seen with E-gold  
12 that there was -- well, I guess, a seizure and  
13 arrest and that there were seizures for -- and  
14 arrests for virtual currency -- or sorry,  
15 operating as a money transmitting business and  
16 also money laundering.

17 Now, the -- in order to prove money  
18 laundering you need to prove that the people who  
19 moved the funds actually have some sort of  
20 knowledge of the funds -- of the origins of the  
21 funds that they're actually moving. Now,  
22 Liberty Reserve came in and actually tried to  
23 modify their plan in order to evade police in  
24 that they were not dealing directly with cash  
25 money or fiat money. Liberty Reserve was

1 virtual currency that was established in Costa  
2 Rica in 2006, and they were reported to be  
3 backed by gold.

4 Now, you could log into the Liberty Reserve  
5 site and you could create your own account, but  
6 you could not deposit fiat money directly into a  
7 Liberty Reserve account. What you could do,  
8 however, is send money to a broker who would  
9 then -- a third-party broker who would then  
10 deposit Liberty Reserve into your Liberty  
11 Reserve account, meaning that Liberty Reserve  
12 would not actually be handling physical fiat  
13 money or you would not be sending money directly  
14 to them. There were also located offshore.

15 So they were part of -- well, I should  
16 mention before that that in 2012, 2013, there  
17 was a modification to the Bank Secrecy Act in  
18 the United States which meant that virtual --  
19 well, companies dealing in virtual currencies  
20 were now recognized as money service businesses  
21 and obliged to obey the laws on reporting and  
22 operating as a money service business.

23 Now, in 2013/14 Liberty Reserve was  
24 indicted, a \$6 billion indictment with  
25 several million dollars seized. And the

1 operator of Liberty Reserve had admitted to  
2 laundering between 200 and \$500 million through  
3 the course of their operations.

4 Now, what we can see is a variation on a  
5 theme; right? So, I mean, rather than starting  
6 another virtual assets company within the United  
7 States, they started it overseas. Rather than  
8 dealing with actual fiat money and potentially  
9 being accused of money laundering, they were  
10 dealing simply with virtual currency, which  
11 didn't mean anything or had no actual intrinsic  
12 value to anyone. And by dealing with a broker,  
13 a middleman, then they could simply say that  
14 they had no involvement or had no way of knowing  
15 who was actually behind the funds that were  
16 actually being transacted.

17 So fast forward, 2013/14. We now look at a  
18 considerable rise in the value of bitcoin which  
19 had been around since 2009; right? And so  
20 bitcoin by itself automatically responded to the  
21 issues of the first two major virtual assets or  
22 virtual currencies which were used to launder  
23 funds. So immediately now you're looking at a  
24 decentralized network, meaning that police  
25 cannot simply go to one -- a one-stop shop and



1                   seize all of the accounts belonging to all of  
2                   the clients. It provided anonymity at the time,  
3                   especially. There were no tools and there was  
4                   no additional means to aid police with tracking  
5                   down who was actually responsible for a  
6                   particular transaction.

7                   So -- well, that anonymity in addition to  
8                   the redundancy of the network as well as not  
9                   requiring a licence, not requiring a money  
10                  service business licence in order to deal with  
11                  bitcoins, really made them popular suddenly  
12                  overnight with those people who had lost  
13                  considerable amounts of money with Liberty  
14                  Reserve and E-gold.

15                 Next slide, please. Okay. So as far as  
16                 bitcoin scams go, I mean, we had discussed these  
17                 previously, but this is to give you an idea of  
18                 how much money can actually be siphoned through  
19                 this particular type of scam, CRA-type scams,  
20                 where we are talking about, you know, a total of  
21                 \$340,000 in the York Region. So we are talking  
22                 about prevalence. Next slide, please.

23                 Ransomware. So this is hopefully a screen  
24                 that you've never actually seen yourself. But  
25                 ransomware is a type of malware that once it

1 affects the system of the victim, it encrypts  
2 their entire -- or all of the data or targeted  
3 data on their computer. In order to regain  
4 access to their data, their only personal  
5 information, they have to pay a certain ransom,  
6 typically paid via bitcoin. And as we saw  
7 before, it's relatively easy to identify a  
8 bitcoin ATM, a location. And so when somebody  
9 calls -- a lot of these -- I should say a lot of  
10 these ransomware pages come with a 1-800 number  
11 and you would call and actually speak to a  
12 receptionist or someone who will answer your  
13 call and actually walk you through the process  
14 of getting back your data and they will search  
15 for bitcoin ATM with you and tell up to go to  
16 the nearest bitcoin ATM, how to buy it and how  
17 to actually transfer to decrypt your files.  
18 Next slide, please.

19 Phishing. We've seen many types of -- many  
20 types of phishing scams. I'm sure that we have  
21 all had those in our email boxes where people  
22 purport to have obtained our password of some  
23 type, some type of extortion, sextortion scams,  
24 CRA scams, basically enticing people -- or  
25 convincing someone that they've actually been a

1                   victim of -- or that they are responsible for  
2                   some type of crime, and then having to pay legal  
3                   fees through bitcoin or through some of other  
4                   mode. Next slide, please.

5                                 Now, we are getting into more of the  
6                   cybercrime types of attacks. So this would be a  
7                   DDoS attack, or distributed denial of service  
8                   attack, and essentially that's a process of  
9                   flooding a network with traffic so that whatever  
10                  site is hosted on that network cannot actually  
11                  operate any longer. So it may not seem like  
12                  that big a deal, but if you're thinking of, you  
13                  know, a network that -- for example, an online  
14                  gambling site which supplies services to however  
15                  many thousands of clients and transacts how many  
16                  thousands of times per hour and you down that  
17                  network for half an hour or more, then you're  
18                  talking about considerable losses for that  
19                  company. And these types of attacks can be paid  
20                  via bitcoin and remain completely anonymous  
21                  going forward.

22                  Q         That's basically another variation on a  
23                  shakedown where the provider company would have  
24                  you as being taken offline and told, pay up  
25                  until -- unless you want to be kept offline?

1           A     (AG) Yes.  So that can be a ransom attack.  It  
2                    can be trying to convince them to actually take  
3                    some sort of action in the interest of whoever  
4                    the person who is attacking.  So it could be any  
5                    number of reasons.  I've seen it for video  
6                    games.  Somebody wants to really win a video  
7                    game and simply takes the network offline.  
8                    Everybody has their motives.  Next slide,  
9                    please.

10                         Infrastructure.  So I can speak as an  
11                         investigator that it's already difficult enough  
12                         to track down cybercriminals.  Now, there was  
13                         the -- there was legislation that was introduced  
14                         in Europe which actually limits the amount of  
15                         information that is required to be put online in  
16                         relation to domains that are being hosted.  But  
17                         in addition to that not being able to find out  
18                         who's behind a particular website that could be  
19                         mirroring a legitimate site or some sort of site  
20                         that's hosting malware or something like that,  
21                         people can host sites or pay for the hosting of  
22                         sites via bitcoin or via another cryptocurrency  
23                         and actually avoid providing any type of  
24                         personal information whatsoever.  And many of  
25                         these sites are hosted offshore, though some are

1                   hosted in Canada, and once again you run into  
2                   the problem of obtaining that information via  
3                   mutual legal assistance treaties and so forth  
4                   and so on. Next slide, please.

5                   Q     And, Acting Sergeant Gilkes, you're now at quite  
6                   a good trot I appreciate because I think I've  
7                   got, on my math for participants' questions and  
8                   such, about a half hour. And your colleague  
9                   Sergeant Krahenbil has been mercifully relieved  
10                  of questions, but I actually will have a few for  
11                  him too as we get towards the end of the slides.  
12                  So I appreciate you covering this ground as you  
13                  are. Carry on.

14                  A     (AG) Okay. Thank you. This is basically a  
15                  basic structure of a money-muling network. So  
16                  if we were to take into account the  
17                  cybercriminal who's on the right there, if he  
18                  were to breach an account via stolen credentials  
19                  or something like that at a particular bank, the  
20                  best way of getting the money out of that bank  
21                  would not actually be to transfer the funds  
22                  directly but to transfer the clients within the  
23                  bank itself. So they attempt to run a network  
24                  at multiple banks, and rather than having the  
25                  funds sent interbranch initially it's sent to

1 multiple clients of -- within that particular  
2 bank.

3 Now, these money mules in this case are  
4 required -- sorry, are recruited in various  
5 ways. So now we've seen those work from home  
6 emails where they say that -- where people will  
7 claim that you can get paid for processing  
8 transactions, so you will be receiving a certain  
9 amount of money a certain number times per day  
10 or per week or what may be, and your job is to  
11 actually withdraw those funds from your account,  
12 buy bitcoin with it and then transfer it back to  
13 whoever actually conducted the data breach or  
14 whoever actually was the cybercriminal to gain  
15 access to the breached account in the first  
16 place. So it's more of a variation on a theme.

17 Next slide, please. Okay. So we'll go  
18 over this briefly. So typically when we mention  
19 the dark web or we mention cryptocurrency, we  
20 mention them synonymously; right? And to give  
21 you an idea of what it is, the surface web is  
22 where most of us deal or where most of us  
23 interact with the internet, so Wikipedia,  
24 Google, et cetera. But most of the internet is  
25 actually contained in the deep web. And so

1                   those are -- that's information that we really  
2                   don't want to have indexed, we don't really want  
3                   to have people to simply be able to Google our  
4                   medical records and, you know, access them  
5                   directly. We -- these are accessible typically  
6                   via portals or computers that are accessible to  
7                   the internet and require some sort of access  
8                   code, email, password, so forth and so on.

9                   And then at the very bottom we have the  
10                  dark web. Now, the dark web, we do hear about  
11                  it often, but it's actually a very, very small  
12                  portion of the internet and it's basically kind  
13                  of an alternate internet which is hosted on  
14                  voluntary computers, and it's -- it is  
15                  encrypted. It's very difficult to trace traffic  
16                  coming to, from or through that internet.

17                 Next slide, please. So now if we take a  
18                 look at the sites that are hosted on the dark  
19                 web we can say that between 50 and 70 percent of  
20                 them are actually illegal, and we're thinking of  
21                 the types of things that you can do on the dark  
22                 web, so that's buy drugs, child exploitation  
23                 material, so forth and so on. But as it was  
24                 initially designed for encrypted communication  
25                 and to permit people to communicate with each

1                   other and at the same time avoid detection and  
2                   avoid eavesdropping, there are still a number of  
3                   legal sites which are on there and people do  
4                   use. For example, reporters trying to spread or  
5                   trying to transmit a message without it actually  
6                   being intercepted and taken down.

7                   Next slide, please. We often hear about  
8                   dark markets on the darknet and the original  
9                   dark market would be Silk Road. Now, Silk Road  
10                  was -- I would call it similar to eBay but  
11                  selling very -- or selling illicit products on  
12                  the site. So you would be able to buy drugs,  
13                  guns, child exploitation material, things like  
14                  that completely anonymously. Now, what's so  
15                  novel is not necessarily that it's basically  
16                  like an illicit eBay, it's actually the payment  
17                  structure. So next slide, please.

18                  So, now, the payment system is what's novel  
19                  about Silk Road because what we were looking at  
20                  were buyers purchasing their bitcoin, so  
21                  typically at that time since we're talking about  
22                  2012, 2013, they were doing it via an exchanger  
23                  or some type of broker who was providing this  
24                  service and getting -- buying the bitcoins for  
25                  them.



1                    Now, the buyer themselves would visit the  
2                    so-called website and see something that they  
3                    would like to purchase, some type of illicit  
4                    substance that they might intend to purchase,  
5                    and they would send the transaction -- send  
6                    those bitcoins to Silk Road. Now, Silk Road  
7                    would hold the bitcoins in escrow and wait until  
8                    the actual product was delivered to the  
9                    purchaser. So once the -- once that purchaser  
10                   has actually received what he had ordered he  
11                   confirms the order to Silk Road who then  
12                   releases the funds minus a commission to the  
13                   vendor, and we finish the cycle.

14                   And the reason this is important is because  
15                   if you are a person who is looking to commit a  
16                   crime, likely you are going to be interacting  
17                   with a criminal and so the level of trust has  
18                   dropped to virtually zero. So enable -- so  
19                   allowing people to have a full trust network, it  
20                   was novel.

21                   Q    Yeah, it regularizes their dealings in the sense  
22                   of providing some -- almost like a third-party  
23                   assurance that the money won't be handed over  
24                   without you getting what you've ordered from  
25                   that illicit menu.

1           A       (AG) Precisely. Okay. So we fast forward to  
2                    2017. And this is where I'd like to make it  
3                    clear that Canada is a player in these types of  
4                    scenarios. So AlphaBay was a kind of Silk Road  
5                    on steroids. I hate to use the term, but it  
6                    was, and it was a very large marketplace run on  
7                    the dark web, which was run by a Canadian. So  
8                    he was an administrator, Alexandre Cazes, and he  
9                    was arrested back in 2017 in Thailand. And as a  
10                   result of this seizure -- or of this arrest  
11                   there was seizure of -- from him from about  
12                   1,600 bitcoin, which I know I had the  
13                   approximate value of about 16,000 -- sorry,  
14                   \$16 million, but currently today's value is  
15                   \$38 million, so that would have to be corrected.  
16                   There was also various properties, high priced  
17                   vehicles which were also seized at that time.

18                                So we can see that there are serious  
19                   Canadian players who are laundering funds and  
20                   providing services on the dark web. Next slide,  
21                   please.

22           Q       This slide gives us a sense of what was on offer  
23                   at the AlphaBay Market.

24           A       (AG) Precisely. So next slide, please.

25                                Okay. So in preparation for the commission

1                   what I did was I actually went to visit the dark  
2                   web and prepared to make purchases as though I  
3                   had never been there before. So basically I  
4                   went on the clear web and I downloaded a dark  
5                   web guide, and the dark web guide basically  
6                   provided me with every -- with instruction on  
7                   everything I would need to be able to purchase  
8                   any number of illicit goods on the dark web.

9                   Now, what I did was after downloading the  
10                  guide it instructed me to install a virtual  
11                  private network, install particular software  
12                  required to navigate the dark web, create an  
13                  encrypted email account in order to be able to  
14                  deal with the individuals. And also I had to  
15                  procure bitcoins, or in this case any type of --  
16                  well, particular cryptocurrency.

17                 So what I did was I registered -- well, I  
18                 created an account at a popular online  
19                 exchanger, bitcoin exchanger, with very minimal  
20                 KYC. And the reason I was able to do that with  
21                 minimal KYC is because I had no intention of  
22                 depositing fiat. Now, if you intend to deposit  
23                 fiat, you tend to have greater requirements in  
24                 terms of reporting on your identity and so forth  
25                 and so on. But in this case I had no intention

1                   of depositing fiat. What I did was I went to an  
2                   ATM machine and I deposited funds directly to  
3                   that online exchanger. Once I deposited to the  
4                   online exchanger I converted from bitcoin to  
5                   Monero, which is a privacy coin which does not  
6                   have a public blockchain. I navigated to the --  
7                   through the dark web using, I guess, a listing  
8                   that was very similar to a Wikipedia-type  
9                   listing for the dark web, and I visited multiple  
10                  sites and prepared to make multiple types of  
11                  purchases.

12                         So of the things that I was able to  
13                   purchase but I did not would be, for example,  
14                   various types of malware, various  
15                   money-laundering instruments, prepaid gift  
16                   cards, so forth and so on, as well as many  
17                   different types of drugs.

18                         I have to mention that in doing so the --  
19                   there was more difficulty in procuring something  
20                   like fentanyl, and based on the chats and the  
21                   forums on these particular sites it was because  
22                   of the -- well, the sites that do sell fentanyl  
23                   garner quite a bit more police attention than do  
24                   sites that don't. Also they tend to try to stay  
25                   away from risks which may actually kill an

1 individual, and there's a high kill rate of  
2 fentanyl. They -- well, at least those were the  
3 reasons given on the sites themselves.

4 Q I wonder if I can interrupt you, Sergeant  
5 Gilkes, to ask you this, though. I appreciate  
6 what you're saying that the -- your recent  
7 attempt to sort of test and have a look at how  
8 quickly and how easily this played out when you  
9 look at the question of fentanyl or fentanyl  
10 precursors that presently seems to have been  
11 more clamped down and so forth, but could you  
12 tell us a bit more about the use of -- whether  
13 it's the use of virtual currencies and/or the  
14 dark web in relation to fentanyl precursors in  
15 particular and that market.

16 A (AG) Well, I think actually Sergeant Krahenbil  
17 might actually be more placed for fentanyl  
18 precursors and fentanyl itself.

19 Q Maybe we can do a little diversion to ask him  
20 that very question, if he -- if I can do that.  
21 I think it's timely.

22 A (WK) Sure. We -- as a group we haven't delved  
23 into fentanyl precursors ourselves online. But  
24 as far as fentanyl being difficult to find, it  
25 hasn't really been because everything that we've

1                   processed has always been fentanyl -- or sorry,  
2                   the items that we've ordered have been fentanyl.  
3                   So precursors I can't speak to, but fentanyl is  
4                   alive and well online.

5           Q       And tell us a bit more about how this connects  
6                   with the use of virtual currency as opposed to  
7                   cash -- like, fiat currency transactions.

8           A       (WK) When products are ordered online, generally  
9                   opioids like OxyContin and the heroins of the  
10                  world, when they arrive, they're generally  
11                  always fentanyl. So we use or --- sorry, when  
12                  you purchase with cryptocurrency and you get the  
13                  product, you're going to be anonymously  
14                  receiving fentanyl in the mail.

15                         When it comes to larger amounts, I mean, we  
16                         have experience in the past where dark web  
17                         traffickers of pure fentanyl were ordering  
18                         specifically large amounts of fentanyl from  
19                         China, having it arrive in Canada, breaking it  
20                         down and selling it via the dark web with  
21                         cryptocurrency, taking that profit from those  
22                         transactions and doing the loop, converting it  
23                         into fiat via prepaid business cards like  
24                         Sergeant Vickery described earlier.

25           Q       All right. Why don't I return to Acting



1                   laundering practises that they can employ to be  
2                   able to help obfuscate that source of funds.

3                   Next slide, please.

4                   So here is just a graph with a list of some  
5                   of these practises that we've identified over  
6                   the course of our investigations, and I'll go  
7                   through each one of them over the next slide.  
8                   So if we can just move on to the next, please.

9                   So first and foremost, unregulated  
10                  exchanges. As I mentioned on a previous slide,  
11                  there's nothing preventing somebody from going  
12                  online and specifically seeking out an exchange  
13                  in another jurisdiction that doesn't need to  
14                  comply with any KYC reporting requirements or  
15                  any AML requirements. There's also the ability  
16                  for the peer-to-peer transactions, so back to  
17                  that initial slide where, you know, buddy's  
18                  wearing a trench coat offering to sell  
19                  cryptocurrency within. This really does provide  
20                  a mechanism just to exchange cash for  
21                  cryptocurrency and have no trace for it.

22                  We can also, you know, pay with prepaid  
23                  cards or gift cards where there's no method to  
24                  be able to trace the source or origin of them.  
25                  As well as just providing private keys offline,



1                   like I mentioned in a previous example.

2                   And then there's the online gambling and  
3                   gaming sites. So there's many of them that  
4                   exist online where you can go in and you can buy  
5                   in basically using cryptocurrency, play a couple  
6                   of rounds and then be able to cash out at any  
7                   point. Now, when you cash out you're provided  
8                   with the reserves that you had put in or at  
9                   least what's left of your pot, but you're not  
10                  necessarily getting back the same cryptocurrency  
11                  that you've put in there, which effectively  
12                  enables you to clean your funds going through  
13                  there. So it's certainly an effective method to  
14                  be able to clean your money.

15                  We'll move on to the next slide, and Acting  
16                  Sergeant Gilkes can go through the process.

17                  (AG) So I will mention that for online  
18                  gambling you can deposit directly from an ATM to  
19                  your online account with whatever gambling site  
20                  there may be. Now, this is actually a scenario  
21                  that I do use for my classes where you go to an  
22                  ATM to deposit directly to a gambling site,  
23                  conduct some transactions. Now, the benefit, I  
24                  suppose, for criminals to possibly use this as  
25                  an alternative would be that it's possible to

1                   win money. So they may actually win money while  
2                   laundering their funds, then the funds can be  
3                   transferred to another address entirely, another  
4                   account and there would be no connection really  
5                   between that initial fiat deposit and the  
6                   bitcoin that ends up into a third party or a  
7                   criminal's account. Next slide, please.

8                   (AV) So on this slide you'll find again  
9                   listed ATMs and prepaid cards. I think that  
10                  we've gone through that to a good extent, so I  
11                  won't beat it to death, which leads us to the  
12                  last point, which is GoFundMe. This is a  
13                  crowdfunding initiative where somebody can  
14                  create an account and solicit donations from  
15                  individuals. We see it oftentimes in order --  
16                  if somebody's ill or -- you know, and needs to  
17                  go to Disneyland for the last time, or various  
18                  such initiatives. So this is a threat, as far  
19                  as I'm concerned, when it comes to  
20                  cryptocurrency transactions. The reason being  
21                  is there's no limit on how many addresses that  
22                  somebody can hold and there's no limit on how  
23                  many wallets they can hold as well. So  
24                  technically if I were -- if I were a bad actor  
25                  and I wanted to launder my funds, I could create

1 a GoFundMe page and start funneling transactions  
2 from my various addresses that I have as well as  
3 maybe co-mingle them with some authentic  
4 transactions, donations from kind members of the  
5 public. At the end of the day I'll have, you  
6 know, a large reserve of cryptocurrency that's  
7 been donated to me, but I can justify the  
8 reasoning behind that is there's lot of kind  
9 individuals out there that have all donated to  
10 my cause to help send me to Disneyland one last  
11 time before I pass away of cancer, for instance.

12 And there's -- because there's no ability  
13 to identify who the holder of all these  
14 addresses are, that unless it's actually being  
15 investigated by law enforcement, it just -- it  
16 provides a good opportunity. Any target can  
17 say, you know what; I'd love to thank those kind  
18 individuals that funded this initiative for me,  
19 but I can't because, you know, I'm not able to  
20 see who the holder of those accounts are.  
21 Meanwhile it's been myself depositing all that  
22 time.

23 These crowdfundings are certainly something  
24 that we're seeing being employed by terrorist  
25 financing groups. So if you want to the go move

1 to the next slide, please, I'll expand on that.

2 So first -- before I get into how they're  
3 using the crowdfunding, I just wanted to talk  
4 really briefly about the SamSam ransomware scam.  
5 And very much like that slide that Acting  
6 Sergeant Gilkes had showed us with the  
7 ransomware and said if, you know, you need to  
8 able to send funds to this particular address,  
9 or just like the picture, the image in this  
10 slide which will show those foreign fighters  
11 holding that banner with a particular bitcoin  
12 address identified in, saying, if you want to  
13 donate to the cause, please send it to this  
14 address. Well, that's exactly what these SamSam  
15 ransomware scam individuals did. They were able  
16 to extort \$6 million US from various hospitals,  
17 universities and institutions.

18 And the reason that they were -- the US law  
19 enforcement was able to take them down was  
20 because as they extorted cryptocurrency  
21 donations from all these entities, they supplied  
22 the same bitcoin address that they wanted them  
23 sent to. They actually had two different  
24 bitcoin addresses. So using these aftermarket  
25 software tools, law enforcement was able to

1 trace this, provide attribution to it and  
2 identify who their suspects were. It was a  
3 great accomplishment. In fact those two bitcoin  
4 addresses were the first ever to be added to the  
5 OFAC list. But what this did was alert  
6 basically the criminal element that law  
7 enforcement, number one, can trace transactions;  
8 number two, if you provide and use the same  
9 bitcoin address each and every time, then you're  
10 likely to get caught.

11 So very shortly after, al-Qassam Brigades  
12 began a crowdfunding campaign to solicit funds  
13 to support its campaign based on what I believe  
14 was a result of this SamSam ransomware scam.  
15 They wanted to collect donations using a  
16 different method, and they created a website.  
17 So every time somebody wanted to go and donate  
18 to this charity through bitcoin transactions,  
19 they would have to click on a link which would  
20 automatically generate a new bitcoin address  
21 that these transactions would go through. And  
22 they simultaneously created a video -- a YouTube  
23 video telling their supporters why they had done  
24 this as an effort to avoid law enforcement. And  
25 like a step-by-step 1, 2, 3 on how to do this.

1                   Al-Qaeda has recently had a campaign where  
2                   they were using social media platforms to  
3                   solicit charity donations. And within COVID  
4                   this year an ISIS facilitator took advantage of  
5                   the whole pandemic and was purporting to be  
6                   selling PPE equipment online and so was  
7                   collecting all sorts of money and purchases and  
8                   donations for this, and was able to take this  
9                   money to be able to fund and support ISIS.

10                   So in August of this year law enforcement  
11                   actually was very successful in taking down  
12                   these three entities and seizing millions of  
13                   dollars in cryptocurrency assets that were used  
14                   for terrorist financing.

15                   Next slide, please. Okay. So chain  
16                   hopping isn't really something we've discussed,  
17                   but each and every cryptocurrency has their own  
18                   individual blockchain for the most part. Some  
19                   of them will piggyback on other blockchains, but  
20                   for the most part they do. So the flow of funds  
21                   can be seen on that particular blockchain and  
22                   these, you know, aftermarket software tools  
23                   allow us to be able to trace it. But a good way  
24                   to be able to break that flow is to change and  
25                   convert from one cryptocurrency into another

1                   because you're basically hopping from one  
2                   blockchain onto a second one or onto a third  
3                   one, if you want to keep the momentum going.  
4                   And in doing so it helps break that flow and  
5                   make it far more difficult for law enforcement  
6                   to be able to trace even using these aftermarket  
7                   tools.

8                   Now, we've mentioned mixers quite a few  
9                   times here, and this is just basically a  
10                  third-party service that you can hire that will  
11                  allow individuals to pool their funds together  
12                  and they will combine them, mix them together  
13                  basically in a blender. And at the end they  
14                  will be able to return the funds to the sender,  
15                  but the funds that you are receiving after it's  
16                  gone through this mixing process is not  
17                  necessarily the funds that you've put into in  
18                  the first place, which will help, again, to  
19                  break up that attribution.

20                  Now, when we go back to the whole process  
21                  and how exchanges are structured and the fact  
22                  that they will take custodial ownership of those  
23                  private keys and they will remove the majority  
24                  of those funds offline into these cold wallets,  
25                  what they're doing basically is pooling

1                   everybody's funds together. Now, they don't all  
2                   use the same method but the majority of them do  
3                   and in essence are really acting as one of these  
4                   mixers, not purposely, but it's how the system  
5                   goes. So exchanges really a wonderful method to  
6                   be able to mix the flow of funds.

7                   Now, coinjoins are very similar. Whereas  
8                   with a mixer you have to trust your funds with a  
9                   third party, so provide them the private keys  
10                  and they're mixing it all up and you really put  
11                  a lot of trust in this individual, this -- like,  
12                  essentially a criminal entity to be able launder  
13                  your funds for you. So coinjoins have gained  
14                  more in popularity because it's the peer-to-peer  
15                  group that will combine their funds in order to  
16                  be able to mix them up rather than depending on  
17                  that third party to do so on their behalf. Next  
18                  slide, please.

19                  And now here's just a few of the money  
20                  laundering/terrorist financing indicators. And  
21                  you'll see that many of them are very similar to  
22                  what we see with the traditional currency or  
23                  banking system. And that's, you know, the use  
24                  of smurfing and third-party money mules to be  
25                  able to deposit these, frequent deposits or



1                   withdrawals, any behaviour that's, you know,  
2                   outside of the normal behaviour when dealing  
3                   with currency.

4                   Now, one thing in law enforcement that  
5                   we've noticed is prolonged meets in vehicles.  
6                   So with traditional drug exchanges, you know, in  
7                   doing surveillance there would be an ability to  
8                   be -- oftentimes to be able to see movement of  
9                   cash or movement of drugs. And in certain files  
10                  that have been seen across Canada but also out  
11                  in -- by the Dutch is that these individuals are  
12                  now meeting together and they're meeting in  
13                  vehicles for an extended period of time.  
14                  Surveillance teams are watching and they can't  
15                  understand what's happening because there's  
16                  actually no transfer or doesn't appear to be any  
17                  transfer of cash.

18                  Well, one thing that they have noticed is  
19                  that both individuals have a smartphone out.  
20                  And so what appears to be happening is that when  
21                  meeting there is a change, there is a  
22                  transaction occurring but it's occurring on the  
23                  blockchain. And now the individuals are sitting  
24                  in the car waiting for a prolonged period of  
25                  time so that they can actually see that the

1 transaction's been validated by the miners and  
2 appears as a block on the blockchain. And only  
3 when that is done and it's confirmed will the  
4 individuals depart and go on their way. Next  
5 slide, please.

6 (AG) This one is as it states. It's simply  
7 for honourable mention. I actually don't know  
8 of any active investigation or otherwise which  
9 confirms illicit -- illicitly gained or  
10 ill-gotten gained bitcoins used to actually  
11 purchase a home, but we can see that there are  
12 people who are willing to trade bitcoins for  
13 homes. So is this a potential for money  
14 laundering? Well, I cannot confirm, but it does  
15 exist. It is out there.

16 Q There isn't an impediment there that if someone  
17 has that -- their money, their earnings, I  
18 suppose, or elicited gains in bitcoin, let's say,  
19 they have -- there's nothing to stop that being  
20 used to go and make the purchase of real estate?

21 A (AG) Right. Or if you are from a jurisdiction  
22 which has a limitation on how much in terms of  
23 funds can be withdrawn from whatever country or  
24 jurisdiction that you're in but you can convert  
25 whatever amount of money, fiat in your country,

1 to crypto, then you would be able to make that  
2 purchase. Next slide, please.

3 Okay. In terms of investigative  
4 challenges, there are new schemes out there  
5 which have made, I can say as an investigator,  
6 our lives much more difficult. And  
7 traditionally when we're talking about  
8 traditional organized crime we're talking about  
9 a pyramidal-type structure where you have the  
10 boss at the top and then his corporals working  
11 for him and so then so forth and so on as you go  
12 down the list until the very bottom. But  
13 everybody really knows who they're working for  
14 and what particular organization they're part of  
15 and who's actually paying their salary at the  
16 end of -- I'm going to say at the end of the  
17 week; right?

18 Whereas when you have these structures of  
19 where criminals work together but from all over  
20 the world, it can -- well, it contributes to  
21 confusion in terms of when you actually do track  
22 down someone who is responsible for a crime and  
23 then you ask them who do they work for. They  
24 legitimately don't know who they work for. They  
25 receive funds to their bitcoin address or

1                   whatever coin address they happen to be using  
2                   from another address with not necessarily a name  
3                   connected to it. They might be communicating  
4                   via some online forum with each other and that's  
5                   the extent to what they know their implication  
6                   is in whatever crime. Particularly if each  
7                   crime is compartmentalize and everyone is given  
8                   a very small task of a complete bigger -- they  
9                   don't have the bigger picture of what they've  
10                   actually done themselves.

11                                So being able to arrest the guy at the  
12                   bottom and then follow the chain all the way up  
13                   to the top to the boss doesn't work as well as  
14                   it used to because of the anonymous structure  
15                   that -- well, and the removal of trust between  
16                   criminals that is there because as we mentioned,  
17                   you know, these transactions are irreversible.  
18                   So you know that once that amount of bitcoin  
19                   hits your address, well, then it can't be  
20                   reversed. So you can trust whatever -- whoever  
21                   your boss happens to be that you've never met  
22                   will continue making your payments.

23                   Q    I take it another challenge there must be that  
24                   you also have a distributed network model where  
25                   it doesn't need to be the sort of classic -- I

1 think one of the slides had a picture of  
2 Al Pacino and Scarface. It doesn't need to be  
3 Al Pacino with his gang in Miami, what have you.  
4 These could be people that don't even know each  
5 other scattered around the globe, so from an  
6 enforcement point of view how do you go about  
7 trying to connect up people who may not even  
8 know each other or know where the other people  
9 physically are situate?

10 A (AG) Precisely. You are going to --

11 Q Okay. You were going to --

12 A (AG) Next slide, please. Sorry.

13 Q Thanks.

14 A (AG) Okay. As far as RCMP virtual asset  
15 investigations go, we've been investigating  
16 virtual assets at the RCMP, I can speak at least  
17 personally, for approximately ten years, since  
18 the beginning of my service with. And there  
19 have been many successful investigations. And  
20 I'm going to qualify what I mean by "successful  
21 investigations."

22 Now, being responsible for the  
23 investigation from beginning to end, so  
24 identifying whatever crime actually happened,  
25 collecting the evidence and being able to prove



1                   particularly virtual asset investigations, I  
2                   don't really want to qualify them as such  
3                   because I make the -- well, I use the allegory  
4                   that if you pay a hitman with bitcoins, it  
5                   doesn't make it a cybercrime when he commits the  
6                   murder. He is still a hitman, he is still  
7                   getting paid in another format, but the crime  
8                   remains the same.

9                   So we may not know of the implication or of  
10                  the involvement of virtual assets at the outset  
11                  of the investigation. This is something that  
12                  may come up once we actually are fully involved  
13                  in the investigation or towards the end of the  
14                  investigation when we actually do a search and  
15                  seizure and then we find oh, whoa, there's  
16                  actually some wallets here, and then we have to  
17                  deal with them differently. So if we discover  
18                  it early on, we can actually develop some sort  
19                  of tracing and monitoring and things like that  
20                  of the behaviour of the criminal. If we  
21                  discover it only towards the end of the  
22                  investigation, well, then, maybe it might be up  
23                  to Digital Forensic Services to come in and try  
24                  and actually do a seizure of the goods as either  
25                  proceeds of crime or the bitcoin used as -- in

1                   the commission of the offence itself.

2                   Q     How do you actually go about trying to do a  
3                   seizure of bitcoin or a virtual currency?

4                   A     (AG) So there's several different ways. I mean,  
5                   as we mentioned before that they could be kept  
6                   on an exchange itself, and then you would have  
7                   to go through legal paperwork. If not and you  
8                   are doing a search, if, for example, there is an  
9                   indicator that is there is wallet on the system  
10                  or on the phone but that the phone is encrypted  
11                  or the computer is encrypted, we might look for  
12                  another alternative, for example, like a seed  
13                  list, as I mentioned before.

14                  Q     Right.

15                  A     (AG) Which is that list of words. And once we  
16                  obtain that list of words, we can recreate the  
17                  wallet itself and then move the funds out to  
18                  different wallets, which I think Sergeant  
19                  Vickery will speak to later. But there's a few  
20                  different approaches we can take to actually  
21                  get -- gain control of that private key or gain  
22                  control of the wallet to be able to sweep the  
23                  funds out into a Crown-controlled wallet.

24                  Q     I assume that has to happen sometimes very  
25                  quickly. It's not like the classic search



1 warrant at the drug house and you've got a stash  
2 of cash which isn't going anywhere if it's being  
3 seized by the police and held pending the  
4 process and possibly forfeiture, what have you.  
5 But if someone else has the right information,  
6 they could be moving the bitcoin out from  
7 underfoot, so to speak.

8 Sergeant Vickery, you've actually dealt with  
9 or are aware of some of these situations?

10 Sorry, you'll need to unmute. There we go.

11 A (AV) Thank you. Yeah. Absolutely, you've hit  
12 the nail on the head there. We can have access  
13 to these wallets or the seed phrases in our  
14 possession, but basically in essence all we have  
15 is an image of, say, a large stash of bulk cash  
16 and there's other people that have that same  
17 image, and it truly is a race to see who can get  
18 their first. We have absolutely no ability to  
19 control who has -- sorry, my cat's here. No  
20 ability to control who has access to that  
21 information and who can essentially gain access  
22 to that cryptocurrency, so we do need to be able  
23 to get it and take it into custody as quickly as  
24 possible to ensure that it's not liquidated or  
25 transferred.

1           Q     Shall we move to the -- one of the last slides,  
2                    the responses to lessons learned?

3           A     (AV) Sure. Just before we get there I just  
4                    wanted to speak very quickly to our most notable  
5                    file and that, as far as I'm concerned, is a  
6                    file that took place in May of 2018 in which the  
7                    Milton RCMP detachment were able to take down a  
8                    prolific darknet vendor online who was selling  
9                    fentanyl and in doing a after his arrest they  
10                   found out they were able to seize cryptocurrency.  
11                   So these members, despite most of them even just  
12                   learning what bitcoin was in the days leading up  
13                   to this arrest and the actual seizure, were able  
14                   to solicit the assistance of our digital  
15                   forensics unit to go in there and recreate a  
16                   wallet and do the seizure of this  
17                   cryptocurrency.

18                            It was very successful file. It ended up  
19                            in conviction in court and the 22-odd bitcoin  
20                            that were seized were -- which had a value of  
21                            about \$200,000 Canadian was successfully  
22                            forfeited as offence-related property. So it  
23                            was a very successful file it's because these  
24                            members showed ingenuity when going after this.  
25                            And we realized, at least from a national

1                   headquarters level, that the RCMP was deficient  
2                   in our ability at that time to be able to handle  
3                   these investigations and support our members to  
4                   it and that we actually needed to have policies  
5                   and guidelines and training in place in order to  
6                   be able to deal with these effectively.

7                   So shortly thereafter the RCMP identified  
8                   an RCMP identified national cryptocurrency  
9                   coordinator, who is myself, led to put these in  
10                  place and make sure that we could meet the  
11                  operational demands and support the field in  
12                  order to be able to do these investigations. So  
13                  since we have created RCMP guidelines, which  
14                  will direct the membership on how to do these  
15                  investigations and the seizure. We also have  
16                  policies to do that and we have guidelines which  
17                  are a little bit more flexibility for us given  
18                  the evolving and dynamic nature of cryptocurrency.  
19                  And truly, because this is a fairly new  
20                  phenomenon for us in law enforcement, we learn  
21                  each and every investigation that we have. So  
22                  these guidelines will allow us to adapt and  
23                  adjust as we learn the best practices, both  
24                  internally to be able to deal with this but also  
25                  from our international law enforcement partners.

1                   So we offer training at all levels for  
2                   few years now, actually. Two years or so we've  
3                   been offering training, national financial crime  
4                   courses, including a proceeds of crime course, a  
5                   counterfeit course, the financial integrity  
6                   course. Terrorist financing course is also  
7                   being offered, the cybercrime courses offered at  
8                   CPC or PRTC, and on the online undercover  
9                   course. We have put together one-day workshops,  
10                  which we piloted out in the Pacific region and  
11                  in Edmonton and Alberta earlier this year, but  
12                  unfortunately those were put on hold due to  
13                  COVID. So currently we're actually building an  
14                  online cryptocurrency 101 course which will be  
15                  accessible to all RCMP regardless of what  
16                  business line they fall into, whether they're  
17                  federal policing or contract level, will be able  
18                  to access and use these -- this training  
19                  opportunity. And the hope is to be able to put  
20                  that over onto the Canadian Police Knowledge  
21                  Network and make it available to all municipal  
22                  and provincial law enforcement in Canada as  
23                  well.

24                   We have developed several working groups  
25                   and worked in collaboration with other partners

1                   in order to enhance our capabilities to be able  
2                   to do this job. There's a virtual currency  
3                   working group that was created actually back in  
4                   2017, and it was kind of in response to several  
5                   initiatives that were being initiated across the  
6                   divisions by several different business lines  
7                   who were all encountering cryptocurrency in  
8                   their own investigations and they were all  
9                   trying separately to build and enhance their  
10                  capability to be able to investigate this.

11                                So what this working group does is be able  
12                                to bring everybody together regardless of what  
13                                business line that they're in and really take a  
14                                multidisciplinary approach to how best we can  
15                                enforce these -- both investigate and enforce  
16                                these crimes. The National Cybercrime  
17                                Coordination Centre has, you know, really been a  
18                                wonderful partner for all of law enforcement  
19                                here in Canada. The National Police Service,  
20                                and as I had mentioned earlier in the testimony  
21                                they have acquired software tracing tools from  
22                                both Chainalysis and CipherTrace which they've  
23                                disseminated out to law enforcement in Canada to  
24                                help us be able to follow these flow of funds  
25                                and, you know, identify attribution to this.

1                   They also provide support to municipal and  
2                   provincial partners who maybe don't have the  
3                   resources within to be able to do their own  
4                   tracing.

5                   They'll provide the ability to do the  
6                   tracing on their behalf. They'll also do  
7                   deconfliction for all law enforcement and they  
8                   are a conduit to Europol as they have a liaison  
9                   officer currently stationed there in The Hague.

10                  The Canadian anti-fraud centre is also a  
11                  wonderful partner for us. Again, I mean they  
12                  see a huge influx of frauds being facilitated  
13                  through cryptocurrency go through their  
14                  databases all the time. They also have access  
15                  to these software tracing tools provided by the  
16                  National Cybercrime Coordination Centre and they  
17                  are really are the first point of contact for  
18                  the RCMP contract members to be able to do that  
19                  tracing of their fraud files and use them as a  
20                  deconfliction tool to see if these addresses are  
21                  linked to other fraud files across the country.

22                  We have partnerships with our Government of  
23                  Canada partners out there, you know, CRA and  
24                  Department of Finance, FINTRAC, FAMG. FAMG is  
25                  another resource, the Forensic Accounting

1 Management Group that we use all the time. They  
2 also have access to these software tracing tools  
3 and can provide tracing support for some of our  
4 larger tier 1 and tier 2 files.

5 We have international partnerships through  
6 the Five Eyes cryptocurrency operational  
7 readiness group where we are able to really  
8 discuss best practices and trade craft as well  
9 as what these Five Eyes countries are doing in  
10 order to build capacity internally and how we  
11 can leverage that in this international fight  
12 against money laundering.

13 Q You speak about partnerships. I wonder if I  
14 could ask you in particular about something  
15 about Project Participate, if you could describe  
16 what that is and to the extent that you or RCMP  
17 have been involved or contributed to that  
18 undertaking.

19 A (AV) Yes. So Project Participate is basically a  
20 working group comprised of a lot of the private  
21 sector money service businesses, and it's a  
22 joint partnership with -- that they are trying  
23 to increase their ability to be able to be  
24 compliant and to implement proper AML/KYC within  
25 their exchanges in order to prevent money

1                   laundering from going through. So they have  
2                   created different documents in trying to, you  
3                   know, educate the money service businesses out  
4                   there on how best to identify that. The RCMP  
5                   does have a representative that is part of this  
6                   group. Our point of contact is based in the  
7                   Greater Toronto Area where many of these  
8                   exchanges are located.

9                   And through this partnership we've been  
10                  able to work with Project Participate to improve  
11                  our ability in law enforcement to be able to go  
12                  after some of these assets -- or not necessarily  
13                  the assets, but at least identify them and who  
14                  the targets of these transactions are. For  
15                  instance, the money service businesses -- or  
16                  virtual asset service providers that are  
17                  part are of Project Participate were able to  
18                  come up with a list of information that they  
19                  captured during the course of their regular  
20                  business activity and were able to provide this  
21                  list of information to law enforcement so that  
22                  we have a template, some sort of starting point  
23                  in how to go -- find this information with a  
24                  production order.

25                  Obviously, you know, we need to be able to



1                   satisfy the grounds to believe that an offence  
2                   has occurred and get lawful authority from the  
3                   court in order to be able to go after these  
4                   funds, but having this template is certainly  
5                   helpful for us. So I can certainly speak to all  
6                   of these partnerships that we have going and how  
7                   valuable each and every one of them are.

8                   Now, the one partner -- Government of  
9                   Canada partner that I haven't quite mentioned  
10                  yet is the Seized Property Management  
11                  Directorate. So the Seized Property Management  
12                  Directorate has been around for ages. I believe  
13                  they were created in 1993 and were a government  
14                  entity designated to manage all seized  
15                  offence-related property and proceeds of crime  
16                  and to manage those assets on -- sorry, for all  
17                  federally prosecuted cases and to manage those  
18                  assets until they were either ordered returned  
19                  upon no conviction or they were forfeited and to  
20                  dispose of those assets upon forfeiture. So  
21                  they're a wonderful entity that's been used by  
22                  federal policing within the RCMP for 25 years,  
23                  but their services did not extend beyond those  
24                  cases in federally prosecuted court, so our  
25                  contract members were unable to use them, we

1                   were unable to use them for, say, fraud files  
2                   and none of our municipal/provincial partners  
3                   were able to employ their services as well.

4                   And, I mean, they have contracts all across  
5                   the country to be able to store these assets for  
6                   a very limited fee. In Vancouver rates for  
7                   storing, say, vehicles are very expensive. You  
8                   can pay up to \$70 a day to be able to store a  
9                   vehicle in a tow yard, whereas the Seized  
10                  Property Management Directorate has contracts  
11                  already in place and can do so for \$6 a day,  
12                  potentially, or \$10 a day. So they have the  
13                  ability to save the government a lot of money.  
14                  They will also be manage all restrained assets.  
15                  So they can go in and manage a house, make sure  
16                  that that -- you know, the lawn is getting cut  
17                  and that the hardwood flooring isn't being  
18                  removed or all gold faucets aren't being removed  
19                  from the homes, to maintain that asset. Next  
20                  slide, please.

21                  Q    I wonder if I could just pause, though, to pick  
22                        up on this and maybe put it through the prism of  
23                        thinking about it in this province. Sergeant  
24                        Krahenbil, would you able to speak a little bit  
25                        about in "E" Division and in British Columbia

1                   the cybercrimes unit, your involvement in it but  
2                   also the number of people that are there and how  
3                   that is organized.

4                   A     (WK)  I think we stated earlier the unit is  
5                   pretty new.  We started in April right in the  
6                   middle of the first COVID lockdown, so some  
7                   difficulties there.  But we've been at this type  
8                   of work since 2016, so we started in the dark  
9                   web in 2016 as a serious and organized crime  
10                  group working specifically on opioids online and  
11                  trafficking, and that's how we -- with that --  
12                  in that venue that's how we came interested in  
13                  sort of working on cryptocurrency also as  
14                  they're -- dark web, fentanyl and cryptocurrency  
15                  pretty much go hand in hand.  So we're currently  
16                  three regular member and an analyst.

17                  Q     Okay.

18                  A     (WK)  There will be expansion to the unit, so we  
19                  will be growing.

20                  Q     When is that expected to happen?

21                  A     (WK)  Hopefully soon.  I can't say for sure.  
22                  This is just something that's in the process,  
23                  so -- yeah.

24                  Q     Do you have a sense of how big of an expansion,  
25                  or is that all under consideration right now?

1           A     (WK) It's all under consideration right now,  
2                    yes.

3           Q     Okay. All right. Sergeant Vickery, we can  
4                    return to this slide. I think we'll probably  
5                    need to switch over to others asking questions  
6                    before I run them out of time too much so -- but  
7                    you carry on, please. You're muted again.

8           A     (AV) Sorry. Just the two slides left. So  
9                    cryptocurrency seizures. We have -- obviously  
10                   we've talked a little bit about the inability to  
11                   be able to control who has access to these seed  
12                   phrases or the private keys and so until we  
13                   actually can transfer or transact the  
14                   cryptocurrency from one address to one belonging  
15                   to the government under a government-controlled  
16                   wallet, we do not really have access to those  
17                   funds. There's also been a lot of concern and I  
18                   guess history supports the need for oversight  
19                   and due diligence when handling this. We have  
20                   seen cases in the US specifically from Silk Road  
21                   where agents from the DEA and the US Secret  
22                   Service were able to divert funds that were  
23                   seized by the law enforcement agencies because  
24                   they had access to the seed phrases. So when it  
25                   comes to our cryptocurrency seizure we're very

1 diligent in the way that we proceed forward with  
2 them by managing who has access to that  
3 information both in terms of disclosure in  
4 court, by restricting the private key or the  
5 seed phrases and managing the members who will  
6 be doing and conducting that seizure.

7 So as the process goes, we have our Digital  
8 Forensic Services Units who will actually  
9 oversee the seizure conducted by our frontline  
10 members. There will be two of them in doing.  
11 Each of them will have responsibility for  
12 securing half of that seed phrase. So they  
13 would truly have to work collaboratively in  
14 order to be able to combine the seed phrase into  
15 an ability to be able to transact that.

16 And then instead of actually keeping the  
17 seizures in our own custody, we were going to be  
18 employing the use of the Seized Property  
19 Management Directorate. So as I had mentioned,  
20 they've been around and have supported federal  
21 policing for years, but their legislation just  
22 recently changed last year, in June of last  
23 year, which will now allow them to provide  
24 services to all municipal/provincial forces in  
25 Canada. And so we have engaged in an MOU with



1           Q     And a number of these topics you've talked on --  
2                    or talked about, rather, but go ahead, please.

3           A     (AV) Yeah. I would say -- I guess I can turn  
4                    the floor over to Sergeant Krahenbil, if he has  
5                    anything more he'd like to add to the federal  
6                    cybercrime operations group, and if not, we can  
7                    go to PCMLTFA amendments.

8                    (WK) I don't really have anything to add  
9                    unless you have questions about what we do or  
10                   where we were at.

11          Q     I think you've given us a sense of that so far.

12                    So the PCMLTFA amendments which we touched  
13                    on before, additional comments about that  
14                    particularly in terms of the implications from  
15                    the law enforcement point of view.

16          A     (AV) So in my opinion I believe that the  
17                    amendments are a wonderful addition here in  
18                    Canada and far overdue. We certainly need them  
19                    here in order to be able to help regulate and  
20                    oversee the transactions that are going through.  
21                    But I do believe that the criminal element is  
22                    very adaptive, and just like the al-Qassam  
23                    Brigades were able to adopt -- or adapt the way  
24                    that they were accepting cryptocurrency payments  
25                    by, you know, providing a method to create a new

1 address each and every time, I think that these  
2 PCMLTFA amendments will just solicit more  
3 ingenuity when it comes to how these --  
4 cryptocurrency is used. I think probably the  
5 criminals will start flocking more to the  
6 privacy coins, such as Monero, to be able to hide  
7 the flow of funds, knowing not only about the  
8 regulations but also that legal tool -- or  
9 sorry, tools exist that will allow us to trace  
10 those -- the flow of funds. And they're very  
11 limited when it comes to some of these privacy  
12 coins such as Monero.

13 (AG) I would just like to add that I think  
14 we can see through -- well, historically, if  
15 we're talking about E-gold and Liberty Reserve  
16 followed by bitcoin, that regulating away crime  
17 doesn't seem to work in terms of simply  
18 eliminating the criminal element. I mean, we  
19 can limit the way or try to hamper them in terms  
20 of their area of operation, but in terms of  
21 eliminating money laundering through  
22 regulations, I think that would be particularly  
23 difficult.

24 As far as our existing structure goes, I  
25 mean, I think that the courts have been -- have



1                   assisted us greatly in fighting money  
2                   laundering, in fighting cybercrime by being so  
3                   open with the application of different laws.

4                   And I also think that as far as the PCMLTFA  
5                   modifications go, what we're going to see is not  
6                   necessarily that we're going to stop money  
7                   laundering through -- by bad actors, but we're  
8                   going to see money services businesses who deal  
9                   in cryptocurrencies being able to come more out  
10                  into the light and actually being more  
11                  recognized by the general public and by banking  
12                  services, and as a result they will be more  
13                  cooperative and be able to provide more  
14                  information to law enforcement and to other  
15                  government agencies who will aid in the  
16                  combatting of the money laundering that occurs  
17                  through their services.

18                  MR. MARTLAND: Members, thank you very much.

19                  Mr. Commissioner, we have, I think, three  
20                  participants who sought some time for questions,  
21                  and the province first. Ms. Harlingten for the  
22                  province.

23                  THE COMMISSIONER: Yes. Thank you, Mr. Martland.

24                  Yes, Mr. Harlingten.

25                  MS. HARLINGTON: Thank you, Mr. Commissioner.

1                   **EXAMINATION BY MS. HARLINGTEN:**

2                   Q     Good afternoon, panel members. Can you all hear  
3                             me all right?

4                   A     (AG) Yes.

5                   Q     Wonderful. So I think my first set of questions  
6                             is largely going to be for Sergeant Vickery.  
7                             Just by way of context for you, Sergeant  
8                             Vickery. I assume you already know this,  
9                             but the terms of reference for the Commissioner  
10                            allows the Commissioner to make recommendations  
11                            for the regulation of financial institutions,  
12                            money services, including unregulated entities  
13                            and persons who provide banking-like services.  
14                            So with that in mind, I'd like to focus on the  
15                            evidence you gave while speaking to my friend,  
16                            Mr. Martland, about the regulation of public  
17                            exchanges, which sort of follows on something  
18                            Acting Sergeant Gilkes just said about  
19                            regulation being difficult.

20                            But when you were discussions that issue  
21                            with Mr. Martland around third-party public  
22                            exchanges, you stated that -- if I'm quoting you  
23                            correctly, that it distances the funds from the  
24                            source. Do I have that correct?

25                   A     (AV) Yes.

1           Q     And because of that distancing, I think you also  
2                   referred to a third-party public exchange as the  
3                   end of a trace for law enforcement?

4           A     (AV) I may have.  If I did say that, it's not  
5                   necessarily the end of a trace, but it certainly  
6                   does provide an opportunity to gather more  
7                   information.

8           Q     So you can follow the public nature of bitcoin  
9                   up to a certain point with the third-party  
10                  exchange and then it becomes -- you have much  
11                  less visibility after that.  Is that a fair  
12                  understanding?

13          A     (AV) Well, through the results obtained via  
14                  judicial authorization, we will be able to --  
15                  hopefully be able to get some know-your-customer  
16                  information on the holder of that account, but  
17                  we'll also be able to get information from the  
18                  exchange where the transaction went once it's  
19                  left the exchange, which now brings us back to  
20                  the blockchain and ability to continue tracing.

21          Q     Okay.  And so I believe in your evidence you  
22                  also said because of some of the difficulties  
23                  around the visibility with third-party public  
24                  exchanges that some regulating and monitoring  
25                  might be helpful in that particular area.  Is

1                   that a fair summary of what you said to  
2                   Mr. Martland?

3           A       (AV) Yes.

4           Q       And so I understand now since the amendments to  
5                   the act came in to the Proceeds of Crime and  
6                   Financing Act that there are going to be FINTRAC  
7                   reporting and know-your-client requirements for  
8                   some of those money service businesses. But I  
9                   understand also that right now there's no  
10                  licensing or regulation provincially for those  
11                  public exchanges. Is that true to your  
12                  knowledge?

13          A       (AV) I can't comment on that. I'm not sure.

14          Q       No, that's totally fine. I will ask you,  
15                  though, just based on your extensive experience,  
16                  is there anything that you would say would be  
17                  helpful from a law enforcement perspective if  
18                  the province were to establish a new provincial  
19                  regulator for these third-party public  
20                  exchanges?

21          A       (AV) What I feel, in my opinion, would be the  
22                  best process is to eliminate the need for these  
23                  third-party service providers and have our  
24                  Canadian banks actually associate directly with  
25                  the exchanges themselves.



1 provided?

2 A (AV) That I can't comment on because I don't  
3 work at FINTRAC. I do know that, you know, our  
4 best case scenario is to be able to get that  
5 information as quickly as possible. As, you  
6 know, we've said throughout the testimony, there  
7 is a great need to be able to go after and seize  
8 these illicit cryptocurrency assets as quickly as  
9 possible because we just aren't able to control  
10 who may or may not have access to them, so the  
11 quicker that we can get the information, the  
12 better.

13 Q Okay. And the customer identification and know  
14 your clients, those -- would it be fair to  
15 characterize those as more preventative or  
16 mitigation measures?

17 A (AV) I believe so. I do think that -- you know,  
18 I mean they're sort of a necessary practice in  
19 order to be able to, you know, deal with the  
20 regulations that are in play but also, as I  
21 mentioned, just as a method for the entity  
22 themselves to protect against fraudulent  
23 activity.

24 Q Right. And I think you said that the  
25 regulations were long overdue. In terms of the

1                   those preventative measures just from your  
2                   knowledge and experience, are there other  
3                   measures that you would consider helpful as  
4                   preventative for money laundering specifically?

5           A       (AV) Well, I would say that I would like -- if I  
6                   had the choice is that I would like to see  
7                   FINTRAC be able to issue higher monetary  
8                   penalties for non-compliance. And we've seen it  
9                   at, you know, a very large extent out in the US  
10                  where FinCEN has -- you know, I think at one  
11                  point -- I want to say they issued a  
12                  \$250 million penalty on BTCE for non-complying,  
13                  and they were a huge facilitator for money  
14                  laundering and it essentially corrupted the  
15                  entity. I don't want to see, you know,  
16                  exchanges that are facilitating money laundering  
17                  actually, you know, all end up in bankruptcy;  
18                  however, it certainly would be a greater  
19                  deterrent if that threat was there.

20           Q       Thank you. I just have one further question.  
21                   When you were talking about responses and lesson  
22                   learned, Sergeant Vickery, you mentioned that  
23                   there was a successful forfeiture with respect  
24                   to the RCMP investigation. Can I take from that  
25                   evidence that you see a role for civil

1 forfeiture for seized cryptocurrency assets?

2 A (AV) Well -- so it was forfeited criminally in  
3 court as offence-related property. You know, in  
4 the RCMP we're always -- you know, I work in the  
5 proceeds of crime/money laundering course and  
6 we're always teaching as a matter of first  
7 resort is to go after the criminal investigation  
8 and go after those assets criminally. And when  
9 the investigation is completely exhausted, then  
10 yes, I do see a benefit of it going civilly.

11 MS. HARLINGTON: Thank you for answer questions,  
12 Sergeant Vickery.

13 Those are all my questions,  
14 Mr. Commissioner.

15 THE COMMISSIONER: Thank you, Mr. Harlingten.

16 And next I understand we have Ms. Magonet.  
17 Is that -- am I pronouncing that correctly? For  
18 the BC Civil Liberties Association, who has been  
19 allocated 30 minutes.

20 MS. MAGONET: Thank you, Mr. Commissioner.

21 To begin if I could ask Madam Registrar to  
22 please pull up the PowerPoint that we were  
23 reviewing this afternoon as I have some -- my  
24 first questions refer to it. Thank you so much,  
25 Madam Registrar.



1                                   Can everyone hear me okay?

2                   A       (AV) Yes.

3                   THE COMMISSIONER: Yes. Thank you.

4                   **EXAMINATION BY MS. MAGONET:**

5                   Q       Okay. Great. So for the most part my questions  
6                                   are directed to whoever on panel feels best  
7                                   positioned to answer them, so you can make that  
8                                   decision yourself, though I have some questions  
9                                   that will be directed to particular individuals.

10                                   Perhaps as a preliminary question before I  
11                                   start going through the slides, I wanted to ask  
12                                   the panel if they would agree that an  
13                                   individual's financial transactions can in some  
14                                   cases contain very personal information about  
15                                   them and could reveal information related to  
16                                   their politics, their religion, their location  
17                                   and even their sexuality?

18                   A       (WK) I'd agree with that.

19                                   (AG) I would agree with that statement as  
20                                   well.

21                   Q       Excellent. And also would the panel agree that  
22                                   individuals who are not engaged in criminal  
23                                   activity may also have a legitimate interest in  
24                                   financial privacy?

25                   A       (AV) Yes.

1 (WK) I agree with that.

2 Q Thank you.

3 MS. MAGONET: Madam Registrar, if you could please go  
4 to slide 2 of the presentation. Thank you.

5 Q So slide 2 and 3 both refer to bitcoin scams,  
6 and I would just like to ask if the panel would  
7 agree that these stories are about scams and not  
8 money laundering using cryptocurrency?

9 A (AG) I would disagree because the  
10 cryptocurrencies were leveraged in order for --  
11 well, for speed, for ease of use and as a way to  
12 dissuade police officers from continuing an  
13 investigation if they happened to believe that  
14 it would be that much more difficult than simply  
15 finding out what bank account the funds were  
16 transferred to.

17 (AV) As well as any cryptocurrency derived  
18 as a result of that fraudulent activity, any  
19 transaction or conversion of that cryptocurrency  
20 now becomes money laundering.

21 Q Okay. Thank you.

22 MS. MAGONET: Madam Registrar, if you could please go  
23 to slide 11 of the presentation.

24 Q So this slide referred to aftermarket software  
25 tools, and the panel did a great job of

1 explaining how these work and what type of  
2 information can be available using these tools.  
3 I just wanted to confirm that when the RCMP  
4 obtains information with the assistance of  
5 aftermarket software tools like Chainalysis, the  
6 type of information provided may include a  
7 user's IP address; is that correct?

8 A (WK) That's correct.

9 Q And these tools are also able to tie  
10 IP addresses to a list of transactions for that  
11 individual; is that correct?

12 A (WK) I don't personally believe they can tie the  
13 IP to the transactions, like a multitude of  
14 transactions, but I could be wrong.

15 Q Could they tie the IP address to a specific  
16 transaction for that individual?

17 A (WK) They could tie the IP address to the  
18 transaction, yes.

19 Q Great. And would that IP address be linked to  
20 any other information for that individual other  
21 than a transaction?

22 A (WK) Are you talking about, like, private  
23 information or something outside of the  
24 blockchain?

25 Q Either inside or out -- actually I would be

1 interest in both, either information within the  
2 blockchain or not related to the blockchain.  
3 For example, if the aftermarket software company  
4 is integrating other sources of information into  
5 their analysis?

6 A (WK) They do integrate OSINT-type information,  
7 but it's not related to the IP.

8 Q Okay. Thank you. And I wanted to confirm that  
9 when the RCMP obtains data from companies like  
10 Chainalysis or other aftermarket software tools,  
11 they do not first seek a production order, but  
12 rather these companies, when paid, hand this  
13 information over to the RCMP?

14 A (WK) The information that comes from Chainalysis  
15 and CipherTrace isn't something that they hand  
16 over to us. It's more of an interpretive tool  
17 of the publicly available information that  
18 already exists.

19 Q But when Chainalysis provides this  
20 interpretation, I think it was maybe earlier  
21 Sergeant Vickery was speaking to the fact that  
22 this can be advantageous -- or that the  
23 blockchain can be advantageous for the RCMP and  
24 these aftermarket software tools can be  
25 advantageous because unlike going through a bank

1                   where you would need a production order to  
2                   access financial information, in these  
3                   circumstances a production order would not be  
4                   necessary; is that correct?

5           A       (AV) But that's not through the use of these  
6                   blockchain, like, aftermarket software tools;  
7                   that was in relations to the blockchain itself.  
8                   Now, these software tools, they are hosted by a  
9                   server from these companies, but really the data  
10                  that's collected on there is data that is  
11                  collected by law enforcement by searching the  
12                  public blockchain.

13                         Now, they can look at some of the searching  
14                         that's been done to come up with their own  
15                         statistics on trends surrounding the illicit use  
16                         of cryptocurrency, but we actually don't gain  
17                         any information from them that would require the  
18                         use of a production order because it is all  
19                         information that they gather from the analysis  
20                         done by police. And each of these licences are  
21                         designated to a specific law enforcement agency,  
22                         so we cannot see, say, what the FBI is tracing  
23                         on there. We can only see what we are doing  
24                         ourselves.

25           Q       Thank you. That's very helpful. So when

1 Chainalysis or another aftermarket software tool  
2 company is providing analysis to the RCMP, they  
3 are only using data that the RCMP has given to  
4 them; is that correct?

5 A (WK) No. No. The data comes from the public  
6 blockchain. So what we're doing is with those  
7 tools is searching the public data.

8 Q Okay. So then the only data that these  
9 companies are analyzing is data that is  
10 available on the blockchain; they're not tying  
11 it to other data sources. Is that accurate?

12 A (WK) Yes and no. The -- they also include OSINT  
13 data. So if you -- say, I'm using Chainalysis  
14 and I want to search for a specific blockchain  
15 address. I can put that into Chainalysis,  
16 they'll provide me the transaction data and if  
17 they have OSINT data, like open source data from  
18 the internet, related to that specific address,  
19 it will show up.

20 Q Okay. Oh, sorry. Go ahead, Sergeant Vickery.

21 A (AV) If I may, we're not really very -- we're  
22 not privy to the proprietary, you know, work of  
23 these software companies. And I know  
24 Chainalysis will be testifying tomorrow so these  
25 questions may be better directed at them on how

1                   they gather this information.

2                   MS. MAGONET: Thank you very much, Sergeant Vickery.

3                               Madam Registrar, if you could please go to  
4                   slide 27 of the PowerPoint. Thank you.

5                   Q    So this slide lists benefits and drawbacks of  
6                   cryptocurrency for criminals and money  
7                   launderers. Would the panel agree that many of  
8                   the advantages listed here are advantages that  
9                   would also exist for people who aren't criminals  
10                  and may explain why they would turn -- or would  
11                  have an interest in cryptocurrency and as well  
12                  for the disadvantages?

13                  A    (AV) Yes.

14                               (AG) Yes.

15                               (WK) Yeah.

16                  Q    Thank you. And would you also agree that one of  
17                  the disadvantages, specifically traceability,  
18                  may in some ways make cryptocurrency less  
19                  advantageous than cash for individuals who are  
20                  engaged in money laundering?

21                  A    (AV) Yes.

22                  MS. MAGONET: Thank you. If Madam Registrar could  
23                  please go to slide 37.

24                  Q    So this slide looks at the surface web, deep web  
25                  and dark web. I was wondering if the panel is

1                   aware that the Tor encrypted technology used on  
2                   the dark web is also used by individuals living  
3                   in countries that have restrictions on freedom  
4                   of expression to circumvent government's  
5                   censorship. So it has been, for example, used  
6                   in China and Russia by people trying to get  
7                   around censorship?

8                   A       (WK) Absolutely.

9                               (AG) Yes.

10                  Q       And that Tor has therefore been endorsed by many  
11                   human rights organizations as a means of  
12                   promoting free expression?

13                  A       (WK) Yes.

14                               (AG) M'mm-hmm.

15                  Q       Thank you. Is the panel aware that BBC launched  
16                   a mirror website on the dark web to circumvent  
17                   censorship in some countries?

18                  A       (WK) Yes.

19                               (AG) M'mm-hmm.

20                  MS. MAGONET: Thank you. If you could please go to  
21                   the next slide, Madam Registrar.

22                  Q       Slide 38 -- oh, sorry.

23                  MR. MARTLAND: I'll just do this for my friend's  
24                   benefit to make sure that we preserve a very  
25                   meticulous record that when -- I think it was



1                   Acting Sergeant Gilkes said m'mm-hmm two  
2                   different times, I took those as being  
3                   agreements, as a yes. So I'll just have the  
4                   record reflect that. I'm sorry to interrupt my  
5                   friend.

6                   MS. MAGONET: No. Thank you.

7                   Q     So this slide sets out a description of the dark  
8                   web and the type of content you could find  
9                   there. You would agree that what defines the  
10                  dark web isn't that it's exclusively illegal  
11                  content or that its existence is illegal but  
12                  rather that the sites on the dark web are not --  
13                  it can't be indexed by search engines and that  
14                  also that it can only be access using certain  
15                  softwares, configurations or authorizations?

16                  A     (AG) Yes, I agree with that.

17                                 (WK) Yes.

18                  Q     Thank you. And just wanted to confirm. Earlier  
19                  I wasn't sure if I heard you, Acting Sergeant  
20                  Gilkes, when you said that 50 to 70 percent of  
21                  the dark web -- did you say that it was legal or  
22                  illegal?

23                  A     (AG) Well, it's an estimate. Like I  
24                  mentioned -- well, I should have clarified. The  
25                  sites on the dark web are not as constant as,

1                   for example, on the clear web. They are up;  
2                   they're down; they're called the hidden  
3                   services. For any number of reasons why they  
4                   were not constant. So we do see a fluctuation  
5                   of 50 to 70 percent of illegal sites of  
6                   different types.

7                   And once again, I expressed that legality  
8                   depends of course on jurisdiction because some  
9                   of the things which would be considered legal in  
10                  Canada would be considered illegal in some other  
11                  countries and so forth, so there's a variation.

12                 Q    Thank you. Would you agree, though, that  
13                    according to this analysis, and I'm not sure  
14                    which jurisdiction they were looking at, that  
15                    only -- that illegal content -- sorry, excuse  
16                    me -- illegal content only accounted for  
17                    27.8 percent of the dark web and that the rest  
18                    was either legal sites, legal pornography and  
19                    broken links?

20                 A    (AG) That is entirely possible. This is -- this  
21                    site is slightly dated, I should advise. I used  
22                    it simply as a representation of the types of  
23                    content that you can find on the dark web  
24                    itself. So the estimates do change over  
25                    the years and this is, I believe, three years

1                   old or so, so the current estimates would likely  
2                   be different.

3           MS. MAGONET: Okay. Thank you. Madam Registrar, if  
4           you could please go to slide 39.

5           Q     So slides 39 and 42 refer to Silk Road and  
6           AlphaBay. And you would agree that these sites  
7           were successfully shut down by law enforcement?

8           A     (AG) Yes.

9                   (WK) Yes.

10          MS. MAGONET: Thank you. Madam Registrar, if you  
11          could please go to slide 45.

12          Q     This slide refers to ways that individuals who  
13          are engaging in bitcoin transactions can take  
14          measures to provide further anonymity. You  
15          would agree that even legitimate users of  
16          bitcoin who aren't engaged in criminal activity  
17          may want to take measures to anonymize their  
18          transactions?

19          A     (AG) Yes.

20                   (WK) Yes.

21          MS. MAGONET: Thank you. Those are my only questions  
22          about the PowerPoint. Thank you so much, Madam  
23          Registrar, for scrolling through it so  
24          efficiently.

25                   I would now like to pull up the 2015 senate

1 report on cryptocurrency that I circulated on  
2 Friday. And -- thank you.

3 Q And I would first like to ask whether the panel  
4 is familiar with this document or recognizes  
5 this document?

6 A (AG) Yes.

7 (WK) Yes.

8 MS. MAGONET: Okay. Great. Madam Registrar, could  
9 you please go to page 32 of this document.

10 Q So this was a Senate report into digital  
11 currency that was done in 2015. And on this  
12 page -- I think it might be a little further up.

13 Yes. Right there. That's perfect. It says:

14 "The Royal Canadian Mounted Police said  
15 that laws and regulations for digital  
16 currencies should not negatively affect  
17 the innovative benefits that legitimate  
18 users derive from these currencies."

19 You would agree with this statement?

20 A (WK) Yes.

21 (AV) Yes.

22 (AG) Yes.

23 MS. MAGONET: Thank you. And, Madam Registrar, if  
24 you could also go to page 39. Yes, this is  
25 perfect.

1 Q And on this page it says:

2 "The Royal Canadian Mounted Police noted  
3 that legitimate users of digital  
4 currencies can benefit from increased  
5 privacy."

6 You would agree with this statement?

7 A (WK) Yes.

8 MS. MAGONET: Excellent. Mr. Commissioner --

9 THE WITNESS: (AG) Yes.

10 MS. MAGONET: Oh, thank you.

11 THE WITNESS: (AG) Sorry.

12 MS. MAGONET: Mr. Commissioner, would it be possible  
13 to have this marked as an exhibit?

14 THE COMMISSIONER: Yes. That is fine. We'll mark  
15 that as our next exhibit. Madam Registrar, I  
16 think I've lost track.

17 THE REGISTRAR: It's number 254, Mr. Commissioner.

18 THE COMMISSIONER: Thank you.

19 **EXHIBIT 254: Senate Report - Digital Currency:**

20 **You Can't Flip this Coin! - June 2015**

21 MS. MAGONET: Thank you, so much to the panelists.

22 And, Mr. Commissioner, those are my questions.

23 THE COMMISSIONER: Thank you. Now, Mr. Gratl, on  
24 behalf of Transparency International Coalition  
25 you've been allocated 45 minutes, and I'm just

1                   wondering if you anticipate taking that full  
2                   amount of time.

3                   MR. GRATL: I do not.

4                   THE COMMISSIONER: Okay. Thanks. Please go ahead.

5                   **EXAMINATION BY MR. GRATL:**

6                   Q     My first question is for Acting Sergeant Gilkes.  
7                   Your curriculum vitae lists collaboration with  
8                   corporate security of major banks, unofficial  
9                   task forces. Which major banks and what are the  
10                  unofficial task forces?

11                  A     (AG) In terms of unofficial task forces, it was  
12                  more in relation to the recovery of defrauded  
13                  funds. Now, this was in collaboration with  
14                  other police departments and the major banks  
15                  themselves, the five major banks, in that when  
16                  there would be a report of -- and a confirmation  
17                  of defrauded funds, there would be an attempt by  
18                  a group of law enforcement to try to track down  
19                  the funds and provide a venue for recovering the  
20                  funds.

21                  Q     So all five major banks, then?

22                  A     (AG) To my knowledge they were all participants  
23                  in some way, but simply to notify police that  
24                  there was -- well, quickly notify police of some  
25                  sort of fraud or some sort of breach that ha

1                   occurred.

2                   Q     All right.  And does this unofficial  
3                   collaboration have a name?

4                   A     (AG) No.  This was actually some time ago,  
5                   several years ago, and it was really in  
6                   association with investigations that were --  
7                   well, there was often collaboration between the  
8                   various police agencies and simply that there  
9                   would be a notification of some sort of breach,  
10                  and then all police -- the police agencies would  
11                  simply contact each other and ask if there was  
12                  anything in your jurisdiction that could be done  
13                  in order to recover whatever funds may have been  
14                  breached or help in any way.

15                  Q     Sergeant Vickery, you mentioned Project  
16                  Participate, and my notes indicate you saying  
17                  that a lot of the private sector money services  
18                  businesses are involved in that.  I take it that  
19                  includes the chartered banks in Canada, does it?

20                  A     (AV) No, I don't believe that the banks are a  
21                  part of that.  I believe that it's all the newly  
22                  registered virtual asset service providers.  
23                  Those that are actually dealing with virtual  
24                  currency exchanges.  There are Canadian entities  
25                  as well as some of the larger ones within the

1 United Kingdom and the United States as well as  
2 private sector such as Grant Thornton, who I  
3 believe will be testifying either tomorrow or  
4 Wednesday.

5 Q I have that note that Scotiabank is part of  
6 Project Participate; is that correct, or can you  
7 speak to it?

8 A (AV) I cannot speak to that. I don't -- I'm not  
9 familiar with all of the parties. As I said,  
10 our counterpart in the RCMP or my colleague out  
11 in the Greater Toronto Area is the  
12 representative. I've sat in on a couple of  
13 meetings but I'm not familiar with all the  
14 participants.

15 Q All right. And then you're familiar with the  
16 alliance with Bank of Montreal called Project  
17 Protect? Have you heard of that?

18 A (AV) Yes, I have.

19 Q All right. So that involves the Bank of  
20 Montreal collaborating with the RCMP; is that  
21 correct?

22 A (AV) I believe so. I wasn't involved in Project  
23 Protect, so I'm not -- again, I don't know who  
24 all the players are in that.

25 Q Okay. Do you agree with the description of



1 Project Protect as a public/private partnership?

2 A (AV) You know what? I just really don't feel  
3 comfortable commenting on it because I -- I  
4 mean, I've heard the name but I really don't --  
5 offhand without reviewing it in advance, I can't  
6 speak to what it was about.

7 Q Acting Sergeant Gilkes, can you speak to Project  
8 Protect, the public/private partnership with  
9 BMO?

10 A (AG) I cannot. I do not have details as to the  
11 operation itself or the project.

12 Q And, Sergeant Krahenbil, could you speak to  
13 Project Protect?

14 A (WK) Sorry, this is the first I've heard of it.

15 Q All right. Would you agree that the banks are  
16 in competition with cryptocurrency because the  
17 banks own other transfer systems like Interac  
18 and Visa?

19 A (AV) Personally, no, I don't believe that  
20 they're in competition with them at all. I  
21 mean, I think that, you know, other payment  
22 methods are still king. The Bank of Canada did  
23 a report, I want to say last year, I believe,  
24 where they evaluated that only 5 percent of  
25 Canadian citizens were currently dealing in

1                    cryptocurrency. So I think, you know, the use  
2                    of cryptocurrency would have to come a lot  
3                    further before the Canadian banks would feel  
4                    that they were in competition with the  
5                    exchanges.

6                    Q    All right. Sergeant Vickery, do you agree there  
7                    is a growing class of institutional investors  
8                    conducting larger transfers of cryptocurrencies?

9                    A    (AV) Can you rephrase that, please.

10                  Q    Institutional investors account for more than  
11                  half of all purchases of bitcoin, for example,  
12                  above \$1 million. You're aware of that?

13                  A    (AV) No, I can't speak to that.

14                  Q    Okay. So you're not aware of the extent to  
15                  which, say, large banks in Canada are involved  
16                  in the purchase of bitcoin?

17                  A    (AV) No, I'm not.

18                  Q    Are banks in Canada involved in the  
19                  cryptocurrency market as over-the-counter  
20                  brokers for their clients?

21                  A    (AV) I cannot speak to that. I don't know.

22                  Q    Acting Sergeant Gilkes, could you speak to that?

23                  A    (AG) I'm actually not aware of that. I'm sorry.

24                  Q    All right. And, Sergeant Krahenbil, have you  
25                  heard of that?

1 A (WK) Sorry, I haven't.

2 Q Okay. Would you -- would any of the panelists  
3 be familiar with large institutional investors  
4 in bitcoin or cybercurrency in Canada at all?

5 A (AV) No.

6 (WK) No, sorry.

7 (AG) No.

8 Q I take it it's fair to conclude that to your  
9 knowledge the RCMP is not interested in the  
10 cybercurrency activities engaged in by private  
11 banks and large institutions in Canada. Is that  
12 true?

13 A (AV) I wouldn't say that at all. I would say  
14 that we are three individuals of a very large  
15 organization and, you know, we can only know so  
16 much or have, you know, an expertise in such a  
17 large area and perhaps there are other  
18 individuals that could speak to this.

19 Q Sergeant Vickery, you're the cybercurrency  
20 coordinator for the entire RCMP based in Ottawa;  
21 right?

22 A (AV) I'm the national cryptocurrency  
23 coordinator, yes.

24 Q Yeah, so if anybody in the RCMP is qualified to  
25 speak about RCMP involvement in cryptocurrency

1                   that would be you, wouldn't it?

2                   A       (AV)  I --

3                   MR. BRONGERS:  Mr. Commissioner, it's Jan Brongers on  
4                   behalf of the Government of Canada.  The witness  
5                   has answered that she does not feel that she is  
6                   able to answer these factual questions.  These  
7                   witnesses have been asked to appear before the  
8                   commission in order to provide factual  
9                   information about virtual currencies, and I  
10                  don't think it's appropriate for counsel to  
11                  continue with this line of questioning when the  
12                  witness has said that she can't provide an  
13                  answer.

14                  MR. GRATL:  I'm just asking about the scope of her  
15                  competency and if anybody within the RCMP is  
16                  better able to speak to that than the witness.

17                  THE COMMISSIONER:  I think that's a fair question.

18                  THE WITNESS:  (AV)  As I had mentioned, I'm really  
19                  not -- I'm not familiar to be able to provide  
20                  you an answer to that at this point.  IT'S  
21                  certainly something that I can look into and  
22                  come back with an answer for, but I cannot  
23                  answer it at this point in time because I do not  
24                  have the knowledge.

25                  MR. GRATL:

1           Q     Sure.  BUT what I was really asking was would  
2                    there be anybody within the RCMP better  
3                    positioned than you to have that knowledge about  
4                    the RCMP's interest in banks' involvement in  
5                    cybercurrency or large institutional investors'  
6                    involvement in cybercurrency?

7           A     (AV) Would there be somebody?  Well, considering  
8                    that I have no answer for you, I would assume  
9                    that there probably is somebody that would know  
10                   more than me, but I'm unable to provide you an  
11                   answer at this point.  I'm not sure how to alter  
12                   that answer any way.

13          Q     Okay.  Thank you.  I take it that you  
14                    appreciate -- this is for each of the panel  
15                    members.  You appreciate that banks in Canada  
16                    are involved in money laundering, Sergeant  
17                    Vickery?

18          A     (AV) Well, does money laundering flow through  
19                    Canadian banks, yes.

20          Q     Acting Sergeant Gilkes?

21          A     (AG) In terms of banks being used as a tool to  
22                    launder funds, I would agree with that  
23                    particular statement.

24          Q     And Sergeant Krahenbil?

25          A     (WK) Other than things that I know anecdotally

1 from the media, it's outside of my venue.

2 Q All right. I just say this, that it would  
3 appear from the slide presentation that the  
4 primary targets of the cryptocurrency are scams,  
5 frauds perpetrated by cybercurrency, phishing,  
6 including sextortion, purchase of drugs and  
7 gambling; is that right?

8 A (AV) They're some of the offences that can be  
9 facilitated through the use of cryptocurrency,  
10 but I think that, you know, cryptocurrency is  
11 basically a substitution for cash and can be  
12 used to enable all kind of criminality. We also  
13 talked about terrorist financing there as well.

14 Q Right. But you're familiar that HSBC, for  
15 example, was charged for laundering billions of  
16 dollars for Mexican cartels?

17 A (AV) I recall something along those lines. I  
18 don't know the exact amount or really even the  
19 bank that was involved.

20 Q And do you know that Scotiabank was -- recently  
21 ran into some trouble in Costa Rica for being  
22 involved in payment of bribes for a large  
23 infrastructure project?

24 A (AV) That I was not aware of.

25 Q All right. And of course those aren't unusual

1                   circumstances, are they?

2           A       (AV) That I cannot speak to.

3           Q       All right. Can you speak to, from a policy  
4                   point of view, why the RCMP is not casting its  
5                   investigative eye on institutional investors  
6                   involved in large transactions?

7           A       (AV) So my role as the national cryptocurrency  
8                   coordinator is to identify, you know, what tools  
9                   are needed by our operational membership in  
10                  order to be able to conduct their cryptocurrency  
11                  investigations. You're asking me questions that  
12                  are at a far higher level and I think there are  
13                  better people suited within the RCMP, certainly  
14                  of a higher rank, to be able to answer these  
15                  questions.

16          Q       All right. Sergeant Vickery, I understand that  
17                  your primary service provider for the detection  
18                  of -- movement of cryptocurrency is the company  
19                  Chainalysis; is that right?

20          A       (AV) No, that's not necessarily correct. We  
21                  also utilize CipherTrace, and we have an equal  
22                  amount of licences for both.

23          Q       I see. All right. Now, is -- what level of due  
24                  diligence has been conducted into Chainalysis's  
25                  history and its operations?

1           A     (AV) So that would be a question better pointed  
2                   to the National Cybercrime Coordination Centre  
3                   who are the organization that have gathered  
4                   these tools on behalf of law enforcement and  
5                   provided access to these tools to us. They have  
6                   done significant work, I know, in that area, but  
7                   I was not involved in it and so cannot speak to  
8                   it.

9           Q     Who operates that national cybercrime  
10                  organization?

11          A     (AV) I believe it's a joint force operation with  
12                  public safety, the RCMP and some other police  
13                  forces, but I'm not sure to their exact  
14                  structure.

15          Q     All right. What level of investigative scrutiny  
16                  is cast on organizations like Chainalysis?

17          A     (AV) As I had mentioned, the background checks  
18                  and the scrutiny would have come from the  
19                  National Cybercrime Coordinate Centre, but I can  
20                  certainly say that the FBI, HSI, DEA, Europol  
21                  all employ the services of these tools and they  
22                  are certainly considered a valuable partner to  
23                  law enforcement.

24          Q     All right. Chainalysis works by aggregating  
25                  publicly available data about transfers of



- 1                   blockchain and then providing software to enable  
2                   searches of those -- of that publicly available  
3                   data; is that correct?   Maybe Sergeant  
4                   Krahenbil --
- 5           A        (AV) yeah, I'll defer.
- 6                   (WK) I believe that's correct.
- 7           Q        All right.   And, Sergeant Krahenbil, I take it  
8                   you're a great -- you've received personally a  
9                   great deal of training into the Chainalysis and  
10                  its systems?
- 11          A        (WK) Yeah, I've received training from  
12                  Chainalysis and I've participated in their  
13                  Webinars.
- 14          Q        All right.   And if Chainalysis doesn't include  
15                  data in its own proprietary database, I take it,  
16                  then, it would be invisible to the RCMP officer  
17                  using the software?
- 18          THE COMMISSIONER:   Sorry, could you repeat that  
19                  question.   I didn't quite hear it.
- 20          MR. GRATL:
- 21          Q        So Chainalysis has a proprietary database which  
22                  is created by aggregating publicly available  
23                  blockchain data; is that right?
- 24          A        (WK) I would probably pass that question off to  
25                  the Chainalysis people, who I believe are going

1 to be testifying tomorrow or the next day.

2 Q All right. The existing RCMP investigations  
3 have not really extended beyond the commission  
4 of ordinary crimes using cybercurrency as a  
5 medium or a vehicle for the commission of the  
6 crime; is that correct?

7 A (WK) So is your -- just to clarify. Your  
8 question is the substantive offence in most of  
9 these investigations is not the cryptocurrency?

10 Q Well, I mean to say that Acting Sergeant Gilkes  
11 stated earlier that just because you pay the  
12 hitman in bitcoin doesn't turn it into a  
13 cybercrime. Well, the same thing is true for  
14 drug crime; right? SO just because you pay for  
15 the mail order fentanyl with bitcoin, that  
16 doesn't turn it into a cybercrime; correct?

17 A (WK) It would be a more of a cyber-enabled  
18 crime.

19 Q Right. So -- and similarly just because you pay  
20 the ransomware people with bitcoin, that doesn't  
21 turn it into a money laundering kind of offence,  
22 does it?

23 A (WK) I don't investigate money laundering  
24 per se myself, but I'd say that the funds would  
25 eventually be laundered down -- wouldn't it

1                   become fiat?

2           Q     All right.  Are you aware of any requirement  
3                   that any elected public officials declare  
4                   cybercurrency asset ownership as part of ethics  
5                   scrutiny?

6           A     (WK) I don't know that.

7           Q     All right.  Is there any type of asset registry  
8                   in Canada that would require a person within  
9                   Canada to declare ownership of cybercurrency?

10          A     (WK) Not that I know of.

11          Q     Sergeant Vickery?

12          A     (AV) No, I do not believe so.

13          Q     All right.  Acting Sergeant Gilkes, is there  
14                   such a thing, an asset registry for  
15                   cybercurrency?

16          A     (AG) To my knowledge, no.

17          Q     All right.  So in that case is there anything  
18                   that would prevent bribes to public officials,  
19                   either elected or senior civil servants, using  
20                   cryptocurrency?

21          A     (AV) I don't believe so.

22                   (WK) I don't think so.

23          Q     All right.  If cybercurrency is an asset, then  
24                   increases in the value of the asset would  
25                   attract capital gains tax; is that correct?

1           A     (AV) Yes, that's the approach that CRA is  
2                   taking.

3           Q     All right. And what work is CRA doing to  
4                   coordinate the detection of capital gains  
5                   derived from the increases in the value of  
6                   cybercurrency?

7           A     (AV) That would be a question best directed to  
8                   Canada Revenue Agency.

9           Q     All right. So you're not -- you don't know of  
10                  any RCMP work in that regard?

11          A     (AV) No.

12          Q     Okay. Would the -- would an asset registry that  
13                  would include registration of cybercurrency be  
14                  of assistance to law enforcement?

15          A     (WK) Sorry, just to clarify that. You're  
16                  talking about, like, a list of the  
17                  cryptocurrency that somebody would own?

18          Q     Yes, that's correct.

19          A     (AV) I mean, of course it would be helpful to  
20                  law enforcement because any information is  
21                  helpful to law enforcement, but it would also be  
22                  detrimental to our privacy rights here in Canada  
23                  for all the legitimate users of cryptocurrency.

24          Q     I wonder if the panel can comment on the use of  
25                  cryptocurrency to conceal non-payment of income

1 tax.

2 A (WK) I don't think I could speak to that.

3 (AG) Personally I've never investigated  
4 income tax evasion, so unfortunately I cannot  
5 speak to that either.

6 Q I'm thinking of a vehicle -- using bitcoin as a  
7 vehicle for offshore transfer of funds within  
8 Canada.

9 A (AV) I mean, certainly having cryptocurrency  
10 offers or enables a means to be able to put  
11 value towards it; right? And as you said,  
12 transfer it offshore. Unless you're under  
13 investigation by the RCMP or you declare it to  
14 CRA, it's very likely that these -- that the  
15 cryptocurrency can go unnoticed or unidentified.  
16 And so yes, there is a huge threat to be able to  
17 use it for tax evasion or to avoid the payment  
18 of capital gains for any interest that is  
19 accrued while it's in your possession.

20 Q When I'm in court in the Vancouver Law Courts I  
21 like to have coffee in the morning at the Waves  
22 café which houses the first bitcoin ATM machine.  
23 I'm usually there from about 7 o'clock when the  
24 cafe opens to 9 o'clock in the morning when the  
25 free parking runs out, and I go to the parking

1                   lot underneath the courthouse. I never see  
2                   anybody use that machine. Are there any records  
3                   kept about how much of a problem ATM bitcoin  
4                   machines might be?

5           A       (AV) Well, I want to say Chainalysis in their  
6                   spring 2020 report reported that 88 percent of  
7                   all cryptocurrency ATMs funds were sent offshore  
8                   to an international country. Now, whether that  
9                   actually supports the amount of illicit  
10                  cryptocurrency going through, I'm not sure, but  
11                  they certainly are seen as a risky mechanism to  
12                  be able to launder funds.

13          Q       All right. But is the RCMP taking any steps to  
14                  attend to transactions -- cryptocurrency  
15                  transactions originating in Canada or with  
16                  Canadian destinations that are of large amounts,  
17                  like in excess of a million dollars, for  
18                  example?

19          A       (AV) Well, that -- I can't speak to ongoing  
20                  investigations as well as, you know, currently  
21                  some of these investigations are done in covert  
22                  methods that aren't necessarily open. The files  
23                  themselves are restricted and not available to  
24                  all of us to be able to view and see what we're  
25                  currently working on.

1           Q     You're saying I can neither confirm nor deny the  
2                   existence of such an investigation?

3           A     (AV) Yeah, you are.

4           Q     All right. Rather than speaking of specific  
5                   investigations, I wonder if as an institutional  
6                   policy whether the RCMP isn't turning its  
7                   investigative eye more to small players like the  
8                   ATM -- the bitcoin ATMs rather than paying  
9                   attention to the large transactions by  
10                  institutional investors for private equity?

11          A     (AV) So I believe what was, you know, addressed  
12                  in the second slide when we began our  
13                  presentation that while, you know, these CRA  
14                  scams appear at first glance to be very small  
15                  amounts, whether it be \$18,000 or \$2,000,  
16                  collectively this is a multi-million-dollar  
17                  fraud scheme, and the Canadian Anti-Fraud Centre  
18                  has collected more than 5,700 complaints of  
19                  fraud dealing with cryptocurrency. So you can  
20                  imagine the totality of the funds that are  
21                  extorted from victims, innocent victims across  
22                  the country, so I don't actually see that as  
23                  being a small fish.

24                         (AG) Also myself, I mentioned in the way  
25                         that the RCMP conducts its investigations, it

1                   doesn't necessarily start off as a virtual asset  
2                   investigation. So we essentially start an  
3                   investigation into whatever type of crime may be  
4                   the substantive crime, and then follow it as it  
5                   goes, and if it leads to virtual assets, then it  
6                   leads to virtual assets. So we tend to approach  
7                   it in that regard.

8                   Q     All right. The predicate offences that you're  
9                   investigating within the institution, those tend  
10                  to be oriented towards the smaller end of the  
11                  transactions rather than the large aggregate  
12                  amounts; is that right?

13                 A     (AG) Well, in terms of investigating smaller  
14                  transactions versus larger transactions, the  
15                  initial complaint tends to be a portion or a  
16                  small compartment of the overall damage or  
17                  the -- of the aggregate offence. So if we  
18                  attempt to take on an investigation and we're  
19                  lucky enough to be able to find out -- find  
20                  other victims, find other evidence that proves  
21                  that it's part of a much larger endeavour, well,  
22                  then that is great and that's where the  
23                  investigation take us. If not, then we're able  
24                  to basically conduct a smaller investigation and  
25                  bring someone to justice who we were able to



1                   prove have three victims as opposed to the 300,  
2                   well, then we continue to do that.

3                   Q     So there's -- so to your knowledge, though,  
4                   there's no presumption of investigative interest  
5                   or suspicion associated with large transactions,  
6                   say, above a million dollars or some other large  
7                   amount the way there might be for presumptive  
8                   reporting for transfers of cash involving  
9                   greater than \$10,000 under the money laundering  
10                  rules?

11                  A     (AV) So you have to understand that these  
12                  regulations have just come into play here in  
13                  Canada. So unless we're actually investigating  
14                  one of these entities we may never have been  
15                  even made aware of that transactions of this  
16                  level have gone through dealing with  
17                  cryptocurrency. And I think, you know, in  
18                  Canada here we're in a far better position now  
19                  that regulations are in play to be alerted to  
20                  this kind of information through proactive  
21                  disclosures from FINTRAC.

22                  Q     I'm not sure that you understood the nature of  
23                  the question. FINTRAC creates a requirement.  
24                  There's a requirement for financial agencies to  
25                  report all cash transactions of greater than

1                   \$10,000. It automatically goes to FINTRAC.

2           A       (AV) Yes.

3           Q       And there's a requirement to ask questions of  
4                   the person engaged in the transaction. Is there  
5                   anything comparable for transactions involving  
6                   cybercurrency?

7           A       (AV) Well, regulations have just come into play  
8                   here in Canada to have the money service  
9                   businesses report any suspicious transaction  
10                  reports, and I believe it will come into effect  
11                  on June 1st of 2021 where the large cash  
12                  transactions, so anything over and above the  
13                  \$10,000 threshold, will need to be reported as  
14                  large cash transactions.

15          Q       All right. Would it assist the RCMP to have  
16                  greater scrutiny the larger the amount reported  
17                  so that, for example, each time you added a zero  
18                  it would -- a transaction would receive, say,  
19                  ten times the scrutiny?

20          A       (AV) Well, I believe that we have to have faith  
21                  in the money service businesses to be able to  
22                  detect these suspicious transactions or the  
23                  large cash transaction. I mean, they are going  
24                  to be mandated to report all of these to  
25                  FINTRAC, and FINTRAC is the entity assigned to

1                   be able to analyze these and, you know, when  
2                   warranted turn this information over to the  
3                   RCMP. So I believe that all information that  
4                   requires that greater level of scrutiny is  
5                   already being disseminated.

6           Q       Okay.

7           A       (AG) I also don't think it's the actual amount  
8                   of the transaction itself that will garner the  
9                   interest; I think it's the nature of the  
10                  transaction. And once again I come to the  
11                  aggregate potential. I mean, if we're talking  
12                  about 1,000 victims of \$100 each versus one  
13                  \$1,100,000 transaction, I mean, you're looking  
14                  at the same damage in the end. So, I mean, it  
15                  makes more sense to target the investigation  
16                  where you can help more victims in your  
17                  investigation.

18           MR. GRATL: Thank you, those are my questions.

19           THE COMMISSIONER: All right. Thank you, Mr. Gratl.

20                           Anything arising, Ms. Magonet? And please  
21                           correct me if I'm mispronouncing your name.

22           MS. MAGONET: Excuse me. It's pronounced Magonet,  
23                           Mr. Commissioner.

24           THE COMMISSIONER: Magonet. Thank you.

25           MS. MAGONET: And -- no problem. And nothing

1 arising. Thank you.

2 THE COMMISSIONER: Thank you. Ms. Harlington?

3 MS. HARLINGTON: Nothing arising from me,

4 Mr. Commissioner. Thank you.

5 THE COMMISSIONER: Mr. -- sorry. Mr. Martland?

6 MR. MARTLAND: No, thank you, Mr. Commissioner. I

7 think that concludes -- subject to anyone else

8 unmuting to tell us otherwise, that concludes

9 our evidence today. Thank you.

10 THE COMMISSIONER: Thank you to the members of the

11 panel. You are now excused from further

12 testifying.

13 All right. We will adjourn until tomorrow

14 at 9:30.

15 THE REGISTRAR: The hearing is now adjourned until

16 November 24th, 2020, at 9:30 a.m. Thank you.

17 **(WITNESSES EXCUSED)**

18 **(PROCEEDINGS ADJOURNED AT 1:49 P.M. TO NOVEMBER 24,**

19 **2020)**

20

21

22

23

24

25