PROCEEDINGS AT HEARING
OF
NOVEMBER 23, 2020

COMMISSIONER AUSTIN F. CULLEN

INDEX OF PROCEEDINGS

INDEX OF EXHIBITS FOR IDENTIFICATION

INDEX OF EXHIBITS

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

probably see on the screenshare right now. First is -- proposed as the next exhibit, overview report with respect to Quadriga CX.

THE COMMISSIONER: Very well. That will be exhibit 246.

THE REGISTRAR: Exhibit 246.

EXHIBIT 246: Overview Report - Quadriga CX

MR. MARTLAND: Secondly, the overview report, virtual assets regarding the Canadian Securities Administrators guidance.

THE COMMISSIONER: 247.

THE REGISTRAR: Exhibit 247.

EXHIBIT 247: Overview Report - Canadian Securities Administrators Publications on Virtual Assets

MR. MARTLAND: Thank you. Third, the overview report on virtual assets regarding the FATF and DOJ documents.

THE COMMISSIONER: 248.

THE REGISTRAR: Exhibit 248.

EXHIBIT 248: Overview Report - FATF Publications on Virtual Assets

MR. MARTLAND: And finally the overview report on Federal regulation of virtual currencies.

THE COMMISSIONER: 249.

THE REGISTRAR: Exhibit 249.

EXHIBIT 249: Overview Report - Federal Regulation of Virtual Currencies

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

THE WITNESS: (WK) That was just fine.

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

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

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

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

THE REGISTRAR: Thank you. And Sergeant Vickery.

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

THE REGISTRAR: Thank you. And Sergeant Krahenbil.

THE WITNESS: (WK) Warren Krahenbil, W-a-r-r-e-n K-r-a-h-e-n-b-i-l.

THE REGISTRAR: Thank you.

AARON GILKES, a witness called for the commission, affirmed.

ADRIENNE VICKERY, a witness called for the commission, affirmed.

WARREN KRAHENBIL, a witness called for the commission, affirmed.

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

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

THE COMMISSIONER: All right. Thank you.

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

THE COMMISSIONER: All right. Thank you.

EXAMINATION BY MR. MARTLAND:

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

Crime, Proceeds of Crime/Money Laundering Section. Is that accurate?

A (AV) Yes, that's correct.

Q You've served with the RCMP since 2005 in a number of different positions, including Commercial Crime, Serious and Organized Crime Section, Financial Crime Section and the National Security High-Risk Traveller Unit?

A (AV) That is correct.

Q And last five years you've served as the national RCMP Money Laundering/Proceeds of Crime Coordinator at national headquarters and in that capacity providing program governance, training development and policy development; is that right?

A (AV) Yes.

Q Your role includes file review, operational feedback of priority money laundering and cryptocurrency files, and that's a role that really spans the whole country?

A (AV) Yes, that is correct.

Q You also participate in the FATF, the Financial Action Task Force, Europol, and with other international law enforcement, and indeed you lead the RCMP domestic working group on

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

A (AV) Yes.

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

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

A (AV) Yes, I do.

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

THE COMMISSIONER: 250.

THE REGISTRAR: Exhibit 250.

EXHIBIT 250: Curriculum Vitae of Sgt. Adrienne Vickery

MR. MARTLAND:

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

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

at the moment.

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

A (AG) That's correct.

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

A (AG) That is correct.

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

A (AG) That is correct.

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

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

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

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

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

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

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

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

A (AG) I do.

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

THE COMMISSIONER: Yes, 251. Thank you.

THE REGISTRAR: Exhibit 251.

EXHIBIT 251: Curriculum Vitae of Cpl. Aaron Gilkes

MR. MARTLAND:

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

A (AG) Yes. Yes.

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

A (AG) It is, yes.

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

A (AG) Yes, it is.

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

been with the RCMP since 2000?

A (AG) Yes.

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

A (AG) Yes.

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

A (AG) It's fair.

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

Q Sir, you recognize that as your CV?

A (AG) I do.

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

THE COMMISSIONER: Very well. 252.

THE REGISTRAR: Exhibit 252.

EXHIBIT 252: Curriculum Vitae of Cpl. Aaron Gilkes

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

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

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

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

A (AV) That's correct.

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

please be marked as exhibit 253.

THE COMMISSIONER: Very well. 253.

THE REGISTRAR: Exhibit 253.

EXHIBIT 253: RCMP Virtual Assets Slideshow

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

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

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

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

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

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

Now, payment --

Q I'm sorry, carry on.

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

of the bitcoin.

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

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

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

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

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

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

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

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

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

Next slide, please.

MR. MARTLAND:

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

A (AV) Sorry.

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

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

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

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

A (AV) Yes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A (AG) That is correct.

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

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

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

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

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

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

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

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

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

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

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

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

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

transactions to a block.

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

Now, what a miner --

Q Let me just perhaps --

A (AG) Sorry.

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

miners.

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

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

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

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

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

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

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

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

Q Go ahead.

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

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

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

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

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

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

happening are relatively limited.

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

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

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

Q What information is on the public ledger?

A (AG) In terms of information on the public

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Next slide, please.

Q Next slide. Thank you.

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

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

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

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

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

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

Q Okay. Yeah.

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

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

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

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

Q Good. Shall we move to slide number 11?

A (AG) Sure.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

your bitcoins.

Q Thank you.

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

> "Digital wallets are hardware or software that manage keys, addresses, and transactions."

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

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

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

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

Now, in terms of security, a wallet being

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

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

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

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

These are both considered cold storage,

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

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

they tend not be to be so popular.

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

A (AG) Yes.

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

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

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

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

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

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

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

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

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

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

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

A (AV) Sorry. Yeah.

Q No, that's okay. Carry on.

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

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

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

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

client is confirmed.

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

A (AV) That is correct.

Q All right. Carry on.

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

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

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

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

So, you know, of course the international

community was completely shaken.

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

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

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

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

It also begs the question that -- you know,

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

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

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

could be followed by investigators?

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

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

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

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

Next slide, please.

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

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

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

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

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

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

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

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

Next slide, please.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q Yeah.

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

Now, most of these machines will capture an

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

Q Or wear a mask these days.

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

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

A (AV) Sure.

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

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

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

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

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

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

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

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

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

Next slide, please.

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

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

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

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

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

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

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

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

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

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

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

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

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

Next slide, please.

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

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

MR. MARTLAND: Thank you.

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

(WITNESSES STOOD DOWN)

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

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

AARON GILKES, a witness for the commission, recalled.

ADRIENNE VICKERY, a witness for the

commission, recalled.

WARREN KRAHENBIL, a witness for the commission, recalled.

THE REGISTRAR: Thank you for waiting. The hearing is now resumed. Mr. Commissioner.

THE COMMISSIONER: Thank you, Madam Registrar.

MR. MARTLAND: Thank you.

EXAMINATION BY MR. MARTLAND (continuing):

Q Panel members, we were, I think, at slide 23 and now on to 24. And I wonder just before we move into 24, though, if I could pick up on a few questions that have to do with the point about the regulation of the ATMs, and if you're able to comment with respect to the FINTRAC reporting regime, which includes registration and reporting particular kinds of transactions, suspicious transactions, certain compliance measures and so forth, and where things stand with in particular some of these different modes of exchange that you've been describing.

A (AV) So I believe all the money service businesses in Canada that will be dealing with virtual currencies will need to -- or will have had to have registered with FINTRAC as of

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

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

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

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

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

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

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

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

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

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

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

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

Next slide, please.

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

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

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

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

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

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

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

Next slide, please.

Q And this is a New York Times headline dealing with the Facebook proposed cryptocurrency called Libra?

A (AG) That is correct. So Libra was originally a proposal for a blockchain cryptocurrency that was backed by several partnership -- well, partner companies. And of those partner companies -- originally it was Visa and Mastercard. And it was basically to have a backed, I suppose in this case, centralized cryptocurrency, but it was met with quite a bit of resistance. The reason being is that Facebook would have overnight become the world's largest bank. If they -- if we took into account that they have approximately 2 billion users all over the planet. And everybody subscribe to something like Libra, that would be an incredible -- an incredibly sized bank much larger than anyone in the world, and it would have, well, enormous repercussions in terms of the stability of currencies of many countries where people might be switching over to using this type of cryptocurrency, which is backed and supported by these very large groups.

Now, the original proposal did not go

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

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

Next slide, please.

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

Drawbacks of Cryptocurrency For Criminals & Money Launderers."

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

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

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

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

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

It's pseudo anonymous, which is an

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

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

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

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

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

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

Next slide, please. Are you going to go?

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

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

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

part of the Shadowcrew bust.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

multiple clients of -- within that particular bank.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Okay. So in preparation for the commission

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sergeant Gilkes with the slide that we had up, please.

A (AG) Yes. I would just mention that in terms of making the purchases, many of the dark markets themselves actually offered mixing services as you made your purchase in order to try to maintain the anonymity of the person who was actually doing the purchase themselves. So it seemed -- it was really rather -- it was either a mixing service that was being offered or they were offering the use of a privacy coin to make the purchase of the illicit substance. Next slide, please.

(AV) Okay. So we keep coming back to bitcoin, and, again, that just, you know, is based on the fact that bitcoin is really the most commonly used cryptocurrency we've seen in our investigations. And despite its pseudo anonymity there are a lot of anonymizing measures that somebody can employ to enhance the privacy associated with it and that's through the use of the VPNs, proxy servers, going onto the darknet, creating fictitious moniker names in order to be able to transact online.

There's also some other additional money

laundering practises that they can employ to be able to help obfuscate that source of funds. Next slide, please.

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

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

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

like I mentioned in a previous example.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q Okay. You were going to --

A (AG) Next slide, please. Sorry.

Q Thanks.

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

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

that a particular individual in the jurisdiction or otherwise was responsible, and then laying the charge and putting them in jail would be a flow through of, I guess, a traditional-type investigation. But a lot of these investigations involving virtual assets are dealing with individuals, like we mentioned before, which may be -- who maybe don't know each other, maybe don't know where they are and require some different types of approaches to investigations.

So in our implication and these types of investigations we may be tasked with something like in AlphaBay; right? Where we'll be tasked with monitoring type of communication, interception of communication, locating particular targets, conducting a certain type of surveillance, so forth and so on, but we'll have a compartmentalized piece of the investigation which will be part of a greater international investigation which will lead to a takedown itself.

So we have been and we continue to be involved in these types of investigations. As far as considering these investigations,

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

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

the commission of the offence itself.

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

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

Q Right.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Obviously, you know, we need to be able to

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

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

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

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

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

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

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

Q Okay.

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

Q When is that expected to happen?

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

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

A (WK) It's all under consideration right now, yes.
Q Okay. All right. Sergeant Vickery, we can return to this slide. I think we'll probably need to switch over to others asking questions before I run them out of time too much so -- but you carry on, please. You're muted again.
A (AV) Sorry. Just the two slides left. So cryptocurrency seizures. We have -- obviously we've talked a little by about the inability to be able to control who has access to these seed phrases or the private keys and so until we actually can transfer or transact the cryptocurrency from one address to one belonging to the government under a government-controlled wallet, we do not really have access to those funds. There's also been a lot of concern and I guess history supports the need for oversight and due diligence when handling this. We have seen cases in the US specifically from Silk Road where agents from the DEA and the US Secret Service were able to divert funds that were seized by the law enforcement agencies because they had access to the seed phrases. So when it comes to our cryptocurrency seizure we're very

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

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

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

them in the RCMP that they can now manage all of our seized assets, both cryptocurrency assets but as well as any seized or recovered property and do so at a very good price for the government.

Now, they have their own internal policies in place when dealing with cryptocurrency seizures and would be able to manage them properly and safely, as we do. They also have the ability to be able to liquidate these assets within a 24-hour period in order to maintain the value of that asset if it's either ordered returned or forfeited.

Now, when it comes to our cryptocurrency seizures, we will always refer to the cryptocurrency in the amount of -- value of the cryptocurrency and never in comparison to its value compared to fiat, the American dollar or Canadian dollar. And that just protects law enforcement from any change in the value of that asset while it's under our custody. So very much the same process that we use when seizing any -- say, a gold bar. We would seize one gold bar; we would return one gold bar or we would forfeit one gold bar. Next slide please.

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

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

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

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

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

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

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

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

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

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

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

MR. MARTLAND: Members, thank you very much.

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

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

Yes, Mr. Harlingten.

MS. HARLINGTON: Thank you, Mr. Commissioner.

EXAMINATION BY MS. HARLINGTEN:

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

A (AG) Yes.

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

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

A (AV) Yes.

Q And because of that distancing, I think you also referred to a third-party public exchange as the end of a trace for law enforcement?
A (AV) I may have. If I did say that, it's not necessarily the end of a trace, but it certainly does provide an opportunity to gather more information.
Q So you can follow the public nature of bitcoin up to a certain point with the third-party exchange and then it becomes -- you have much less visibility after that. Is that a fair understanding?
A (AV) Well, through the results obtained via judicial authorization, we will be able to -- hopefully be able to get some know-your-customer information on the holder of that account, but we'll also be able to get information from the exchange where the transaction went once it's left the exchange, which now brings us back to the blockchain and ability to continue tracing.
Q Okay. And so I believe in your evidence you also said because of some of the difficulties around the visibility with third-party pubic exchanges that some regulating and monitoring might be helpful in that particular area. Is

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

A (AV) Yes.

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

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

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

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

Q And just to elaborate a bit on that. Is that because those financial institutions are regulated, and so some of the difficulties around knowing what those third-party regulator -- or pardon me, third-party exchangers were doing for a law enforcement?

A (AV) Yes, and in doing so also, I mean, it would help support the purchase of cryptocurrency with, you know, bank transfers and credit cards rather than gift guards or Canada Post or money orders.

Q So if I understand correctly, would it be fair to say that that would bring cryptocurrency into our current financial system rather than creating a regulation for it outside of that financial system?

A (AV) Yes, exactly.

Q All right. And just to return to the FINTRAC reporting requirements, and I understand that those will -- well, those are in force now. Is it fair to stay, though, that those reporting requirements when that information goes to FINTRAC, there is going to be a bit of a time lag between reporting and law enforcement activity with respect to any information

provided?

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

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

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

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

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

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

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

forfeiture for seized cryptocurrency assets?

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

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

Those are all my questions, Mr. Commissioner.

THE COMMISSIONER: Thank you, Mr. Harlingten.

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

MS. MAGONET: Thank you, Mr. Commissioner.

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

Can everyone hear me okay?

A (AV) Yes.

THE COMMISSIONER: Yes. Thank you.

EXAMINATION BY MS. MAGONET:

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

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

A (WK) I'd agree with that.

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

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

A (AV) Yes.

(WK) I agree with that.

Q Thank you.

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

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

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

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

Q Okay. Thank you.

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

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

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

A (WK) That's correct.

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

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

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

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

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

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

Q Either inside or out -- actually I would be

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

they gather this information.

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

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

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

A (AV) Yes.

(AG) Yes.

(WK) Yeah.

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

A (AV) Yes.

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

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

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

A (WK) Absolutely.

(AG) Yes.

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

A (WK) Yes.

(AG) M'mm-hmm.

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

A (WK) Yes.

(AG) M'mm-hmm.

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

Q Slide 38 -- oh, sorry.

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

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

MS. MAGONET: No. Thank you.

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

A (AG) Yes, I agree with that.

(WK) Yes.

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

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

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

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

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

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

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

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

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

A (AG) Yes.

(WK) Yes.

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

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

A (AG) Yes.

(WK) Yes.

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

I would now like to pull up the 2015 senate

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

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

A (AG) Yes.

(WK) Yes.

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

Q So this was a Senate report into digital currency that was done in 2015. And on this page -- I think it might be a little further up. Yes. Right there. That's perfect. It says:

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

You would agree with this statement?

A (WK) Yes.

(AV) Yes.

(AG) Yes.

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

Q And on this page it says:

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

You would agree with this statement?

A (WK) Yes.

MS. MAGONET: Excellent. Mr. Commissioner --

THE WITNESS: (AG) Yes.

MS. MAGONET: Oh, thank you.

THE WITNESS: (AG) Sorry.

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

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

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

THE COMMISSIONER: Thank you.

EXHIBIT 254: Senate Report - Digital Currency: You Can't Flip this Coin! - June 2015

MS. MAGONET: Thank you, so much to the panelists. And, Mr. Commissioner, those are my questions.

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

wondering if you anticipate taking that full amount of time.

MR. GRATL: I do not.

THE COMMISSIONER: Okay. Thanks. Please go ahead.

EXAMINATION BY MR. GRATL:

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

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

Q So all five major banks, then?

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

occurred.

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

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

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

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

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

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

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

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

A (AV) Yes, I have.

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

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

Q Okay. Do you agree with the description of

Project Protect as a public/private partnership?
A (AV) You know what? I just really don't feel comfortable commenting on it because I -- I mean, I've heard the name but I really don't -- offhand without reviewing it in advance, I can't speak to what it was about.
Q Acting Sergeant Gilkes, can you speak to Project Protect, the public/private partnership with BMO?
A (AG) I cannot. I do not have details as to the operation itself or the project.
Q And, Sergeant Krahenbil, could you speak to Project Protect?
A (WK) Sorry, this is the first I've heard of it.
Q All right. Would you agree that the banks are in competition with cryptocurrency because the banks own other transfer systems like Interac and Visa?
A (AV) Personally, no, I don't believe that they're in competition with them at all. I mean, I think that, you know, other payment methods are still king. The Bank of Canada did a report, I want to say last year, I believe, where they evaluated that only 5 percent of Canadian citizens were currently dealing in

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

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

A (AV) Can you rephrase that, please.

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

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

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

A (AV) No, I'm not.

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

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

Q Acting Sergeant Gilkes, could you speak to that?

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

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

A (WK) Sorry, I haven't.
Q Okay. Would you -- would any of the panelists be familiar with large institutional investors in bitcoin or cybercurrency in Canada at all?
A (AV) No.
(WK) No, sorry.
(AG) No.
Q I take it it's fair to conclude that to your knowledge the RCMP is not interested in the cybercurrency activities engaged in by private banks and large institutions in Canada. Is that true?
A (AV) I wouldn't say that at all. I would say that we are three individuals of a very large organization and, you know, we can only know so much or have, you know, an expertise in such a large area and perhaps there are other individuals that could speak to this.
Q Sergeant Vickery, you're the cybercurrency coordinator for the entire RCMP based in Ottawa; right?
A (AV) I'm the national cryptocurrency coordinator, yes.
Q Yeah, so if anybody in the RCMP is qualified to speak about RCMP involvement in cryptocurrency

that would be you, wouldn't it?

A (AV) I --

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

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

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

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

MR. GRATL:

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

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

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

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

Q Acting Sergeant Gilkes?

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

Q And Sergeant Krahenbil?

A (WK) Other than things that I know anecdotally

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

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

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

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

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

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

A (AV) That I was not aware of.

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

circumstances, are they?

A (AV) That I cannot speak to.

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

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

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

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

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

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

Q Who operates that national cybercrime organization?

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

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

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

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

blockchain and then providing software to enable searches of those -- of that publicly available data; is that correct? Maybe Sergeant Krahenbil --

A (AV) yeah, I'll defer.

(WK) I believe that's correct.

Q All right. And, Sergeant Krahenbil, I take it you're a great -- you've received personally a great deal of training into the Chainalysis and its systems?

A (WK) Yeah, I've received training from Chainalysis and I've participated in their Webinars.

Q All right. And if Chainalysis doesn't include data in its own proprietary database, I take it, then, it would be invisible to the RCMP officer using the software?

THE COMMISSIONER: Sorry, could you repeat that question. I didn't quite hear it.

MR. GRATL:

Q So Chainalysis has a proprietary database which is created by aggregating publicly available blockchain data; is that right?

A (WK) I would probably pass that question off to the Chainalysis people, who I believe are going

to be testifying tomorrow or the next day.

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

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

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

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

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

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

become fiat?

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

A (WK) I don't know that.

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

A (WK) Not that I know of.

Q Sergeant Vickery?

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

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

A (AG) To my knowledge, no.

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

A (AV) I don't believe so.

(WK) I don't think so.

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

A (AV) Yes, that's the approach that CRA is taking.
Q All right. And what work is CRA doing to coordinate the detection of capital gains derived from the increases in the value of cybercurrency?
A (AV) That would be a question best directed to Canada Revenue Agency.
Q All right. So you're not -- you don't know of any RCMP work in that regard?
A (AV) No.
Q Okay. Would the -- would an asset registry that would include registration of cybercurrency be of assistance to law enforcement?
A (WK) Sorry, just to clarify that. You're talking about, like, a list of the cryptocurrency that somebody would own?
Q Yes, that's correct.
A (AV) I mean, of course it would be helpful to law enforcement because any information is helpful to law enforcement, but it would also be detrimental to our privacy rights here in Canada for all the legitimate users of cryptocurrency.
Q I wonder if the panel can comment on the use of cryptocurrency to conceal non-payment of income

tax.

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

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

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

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

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

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

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

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

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

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

A (AV) Yeah, you are.

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

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

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

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

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

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

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

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

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

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

$10,000. It automatically goes to FINTRAC.

A (AV) Yes.

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

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

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

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

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

Q Okay.

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

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

THE COMMISSIONER: All right. Thank you, Mr. Gratl. Anything arising, Ms. Magonet? And please correct me if I'm mispronouncing your name.

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

THE COMMISSIONER: Magonet. Thank you.

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

arising. Thank you.

THE COMMISSIONER: Thank you. Ms. Harlingten?

MS. HARLINGTON: Nothing arising from me, Mr. Commissioner. Thank you.

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

MR. MARTLAND: No, thank you, Mr. Commissioner. I think that concludes -- subject to anyone else unmuting to tell us otherwise, that concludes our evidence today. Thank you.

THE COMMISSIONER: Thank you to the members of the panel. You are now excused from further testifying.

All right. We will adjourn until tomorrow at 9:30.

THE REGISTRAR: The hearing is now adjourned until November 24th, 2020, at 9:30 a.m. Thank you.

(WITNESSES EXCUSED)

(PROCEEDINGS ADJOURNED AT 1:49 P.M. TO NOVEMBER 24, 2020)