

**PROCEEDINGS AT HEARING
OF
NOVEMBER 24, 2020**

COMMISSIONER AUSTIN F. CULLEN

INDEX OF PROCEEDINGS

Witness	Description	Page
	Proceedings commenced at 9:30 a.m.	1
	Discussion re procedural matters	2
Jesse Spiro (for the commission) Ian place (for the commission)	Examination by Ms. Rose	3
	Proceedings adjourned at 10:31 a.m.	52
	Proceedings reconvened at 10:40 a.m.	52
Jesse Spiro (for the commission) Ian place (for the commission)	Examination by Ms. Rose (continuing)	53
	Proceedings adjourned at 11:09 a.m.	73
	Proceedings reconvened at 11:15 a.m.	73
Jesse Spiro (for the commission)	Examination by Ms. Rose (continuing)	74
	Examination by Ms. Chewka	108
	Examination by Ms. Magonet	123
	Proceedings adjourned at 12:46 p.m.	142
	Proceedings reconvened at 12:56 p.m.	142
Jesse Spiro (for the commission)	Discussion re witnesses	142
	Examination by Mr. Gratl	143
	Proceedings adjourned at 1:36 p.m. to November 25, 2020	170

INDEX OF EXHIBITS FOR IDENTIFICATION

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

No exhibits for identification marked.

INDEX OF EXHIBITS

No.	Description	Page
255	Curriculum Vitae of Jesse Spiro	5
256	Curriculum Vitae of Ian Place	6
257	Chainalysis - The 2020 State of Crypto Crime report - January 2020	10
258	Chainalysis - The 2020 Geography of Cryptocurrency Report - September 2020	13
259	FATF Report - Virtual Assets Red Flag Indicators – September 2020	72
260	Chainalysis Reactor webpage	166

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

November 24, 2020

(Via Videoconference)

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

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

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

MR. MARTLAND: Thank you, Mr. Commissioner, Ms. Rose has conduct of today's evidence.

THE COMMISSIONER: Thank you, Ms. Rose.

MS. ROSE: Mr. Commissioner, there are two witnesses that we anticipate hearing from today, Mr. Jesse Spiro and Mr. Ian Place, and both work for Chainalysis Inc., a virtual assets tracing company. Madam Registrar, both witnesses have stated they will affirm.

THE REGISTRAR: Witnesses, would you please unmute yourselves. Would each of you please state your full name and spell your first name and last name for the record.

THE WITNESS: (JS) My full name is Jesse Benjamin Spiro. J-e-s-s-e. Last name Spiro, S-p-i-r-o.

THE REGISTRAR: Thank you. Mr. Place.

THE WITNESS: (IP) Ian Michael Place. I-a-n P-l-a-c-e.

1 **JESSE SPIRO, a witness**
2 **called for the**
3 **commission, affirmed.**
4 **IAN PLACE, a witness**
5 **called for the**
6 **commission, affirmed.**

7 MS. ROSE: Mr. Commissioner, as with the evidence
8 yesterday, with the documents for today's panels
9 we have no qualms about them being shared on the
10 webcast. My expectation is that as we go
11 forward we can display both of these on the Zoom
12 and through the live stream.

13 THE COMMISSIONER: Thank you, Ms. Rose.

14 MS. ROSE: I also wish to alert to you the fact that
15 we are assisted today by Mr. Place with a
16 demonstration of the Chainalysis software. So I
17 would first propose to spend some time walking
18 through the witnesses' background, to mark their
19 CVs, and then to ask some preliminary questions
20 about Chainalysis's work before then turning to
21 the demonstration. I expect that I will have
22 some questions for Mr. Spiro following that
23 demonstration.

24 THE COMMISSIONER: Thank you.

25

1 A (JS) That is correct.

2 Q And you are also an instructor for the
3 Association of Certified Anti-Money Laundering
4 Specialists?

5 A (JS) That is correct.

6 Q You have published on various typologies of
7 illicit activity connected with virtual assets
8 such as crypto grey markets and hacking as well
9 as publishing on regulatory developments?

10 A (JS) That is correct.

11 Q And Chainalysis is a company based in the United
12 States?

13 A (JS) Yes.

14 Q And you are joining us today from the
15 Washington, DC area?

16 A (JS) That is correct.

17 MS. ROSE: Okay. Madam Registrar, I'd ask that
18 Mr. Spiro's CV be presented on the screen.

19 Q Mr. Spiro, do you recognize this document to be
20 your CV?

21 A (JS) I do.

22 MS. ROSE: Mr. Commissioner, I would ask that this be
23 marked as the next exhibit, which I believe is
24 exhibit 256.

25 THE REGISTRAR: 255.

1 MS. ROSE: 255, my apologies.

2 THE COMMISSIONER: That will be marked as 255.

3 THE REGISTRAR: Exhibit 255.

4 **EXHIBIT 255: Curriculum Vitae of Jesse Spiro**

5 MS. ROSE: Thank you, Mr. Commissioner. Madam

6 Registrar, I'm finished with this CV. Thank

7 you. Sorry, Madam Registrar, I just ask that

8 you stop screensharing. Thanks.

9 Q Mr. Place, you began working for Chainalysis in
10 May of 2019 as a customer service or Customer
11 Success Manager?

12 A (IP) Correct.

13 Q And your role at that time was to assist clients
14 with technical integrations and provide
15 technical support?

16 A (IP) Correct.

17 Q And you now work as Director of Solutions
18 Architecture, a position you've held since
19 December of 2019?

20 A (IP) Yeah, correct.

21 Q And your role now includes technical integration
22 as it did before but now also includes work flow
23 guides, guidance on best practices in using the
24 Chainalysis software and development of
25 curriculum for Chainalysis training?

1 A Yeah, that's correct.

2 Q And prior to joining Chainalysis you worked in
3 the anti-money laundering, fraud and risk
4 analysis area for an array of financial
5 technology companies?

6 A Correct.

7 Q And through your work at Chainalysis you are
8 adept at using the Chainalysis software to trace
9 virtual asset transactions?

10 A Correct.

11 MS. ROSE: Madam Registrar, could we please have
12 Mr. Place's CV be presented on the screen.

13 Q Mr. Place, do you recognize this document as
14 your CV?

15 A I do.

16 MS. ROSE: Thank you, Madam Registrar.

17 Mr. Commissioner, I would ask in this the CV be
18 marked as the next exhibit.

19 THE COMMISSIONER: 256.

20 THE REGISTRAR: Exhibit 256.

21 **EXHIBIT 256: Curriculum Vitae of Ian Place**

22 MS. ROSE:

23 Q Thank you. Mr. Spiro, could you describe what
24 drew you to the virtual assets space?

25 A (JS) Yeah, so in my previous positions when I

1 was with both Thomson Reuters and Refinitiv when
2 I oversaw threat finance and emerging risks, one
3 of spaces that we began to look into was the
4 emergence of digital payments and specifically
5 cryptocurrencies and the potential risks posed
6 as it pertained to anti-money laundering and
7 countering the financing of terrorism. As I
8 continued to develop my knowledge and capacity
9 around that technology in the space, I also
10 became familiar with some of the providers
11 within the space that were providing forensic
12 services and capabilities, and that is how I
13 became aware of Chainalysis. As I learned more
14 about the capabilities of their products and
15 what they could do in relation to following the
16 flow of illicit funds, it became very attractive
17 to me because I saw a market change in relation
18 to what I saw in relation to traditional
19 financial services. I can -- please.

20 Q Sorry. Could you describe what Chainalysis's
21 products are?

22 A (JS) Yes. So Chainalysis provides blockchain
23 forensics and investigative services. In
24 relation to the products we provide, and we will
25 demo on all three, we provide Reactor, which is

1 an investigative tool allowing investigators to
2 investigate and follow the transaction history
3 and lifecycle in relation to cryptocurrency
4 payments. We have a product that is primarily
5 geared towards compliance purposes which is
6 called KYT for Know Your Transaction wherein our
7 clients from the private sector can integrate
8 with their EAPI and screen their transactions in
9 realtime to identify potential risks in relation
10 to exposure and the transaction history
11 connected to those transactions. And then we
12 have a product called Kryptos which provides
13 market intelligence and specific information in
14 relation to entities that are within the
15 cryptocurrency ecosystem. Those are the
16 products. We also provide services as well.

17 Q I understand that Chainalysis also publishes
18 certain publications. Could you tell me a
19 little bit about those.

20 A (JS) Yes. So we regularly publish different
21 kinds of publications. We put out a cryptocrime
22 report annually where we review all of the on
23 chain data and the information that we've
24 collected to develop and generate new insights
25 that we share with the broader community in

1 relation to trends and other kinds of activity.
2 Recently we provided a geography report which
3 identified and mapped out the cryptocurrency
4 related activity around the globe and some of
5 the trends that we'd seen there. Sometimes we
6 publish specific case studies in relation to
7 certain kind of illicit activity and how we were
8 able to investigate them, different kinds of
9 information we were able to generate. We also
10 produce thought leadership in relation to
11 regulatory developments and how that regulation
12 aligns with different products and services
13 within the ecosystem as well.

14 MS. ROSE: Madam Registrar, could I please have
15 appendix A, a 2020 cryptocrime report on the
16 screen.

17 Q Mr. Spiro, is this one of the cryptocrime
18 reports that you were just discussing?

19 A (JS) It is.

20 Q And are you involved in consulting or authoring
21 on this report?

22 A (JS) I am not the author. I have provided
23 feedback on the report and some feedback in
24 relation to regulation and potential impact it
25 has had in relation to some of the specific

1 insights that we have derived.

2 Q And at a very general level where does the data
3 in these reports come from?

4 A (JS) So in relation to the attributions and the
5 information that we were able to identify we've
6 also been able to identify the jurisdictions in
7 which entities exist, right, and so by way of
8 following the flow of funds we are able to
9 identify where the money is potentially going
10 geographically -- where the money is going, I
11 should say, geographically. So from there we're
12 able to kind of build out and develop insights
13 in relation to strategically what we're seeing
14 in relation to growth and other particulars
15 within different jurisdictions.

16 MS. ROSE: Mr. Commissioner, I would ask that this
17 document be marked as our next exhibit, which if
18 I'm counting correctly we are at 257.

19 THE COMMISSIONER: I think that's right. It will be
20 marked as 257.

21 THE REGISTRAR: Exhibit 257.

22 **EXHIBIT 257: Chainalysis - The 2020 State of**
23 **Crypto Crime report - January 2020**

24 MS. ROSE: Thank you. And, Madam Registrar, could we
25 have the appendix B "2020 Geography of Crypto

1 Report" be put on the screen next.

2 Q Mr. Spiro, do you recognize this document as
3 being the geography of cryptocurrency report you
4 were just discussing?

5 A (JS) I do, yes. I believe I may have made a
6 mistake. I should reference in the cryptocrime
7 report I do also provide feedback in relation to
8 the cryptocrime and the regulatory impact
9 potentially on that, but what I was referencing
10 in relation to the geographic particulars
11 pertains to this report.

12 Q So perhaps I could just ask you to go back and
13 answer my previous question with respect to the
14 cryptocrime report. At a general level where
15 does the data in the cryptocrime report come
16 from?

17 A (JS) Yes. The data in the cryptocrime report
18 also is sourced in relation to what we find on
19 chain in relation to the illicit activity that
20 we were arable to identify and follow. So per
21 the illicit activity that we are able to
22 identify and then the blockchain monitoring and
23 tracing that we are able to conduct, we are able
24 to identify specific volumes and build out other
25 particulars in relation to those kinds of crime

1 typologies and then we share that information
2 accordingly.

3 Q And with this report that's on the screen, the
4 Geography of Cryptocurrency Report, it's
5 primarily from the data that Chainalysis sees in
6 terms of the starting and end point of
7 transactions; is that right?

8 A (JS) Yes. So in relation to the flow of funds
9 and the transaction flow, that's how we are able
10 to identify specific information in metrics in
11 relation to the geographies. Now, I should add
12 that this isn't all encompassing and that what
13 we're following is in relation to entities. So
14 transactions that occur between exchanges and
15 entities within the cryptocurrency ecosystem.
16 In some jurisdictions there is also robust peer
17 to peer activity which potentially is direct
18 activity and interaction between users which
19 would not be accounted for necessarily in some
20 of the geography content that we produce.

21 Q So in both reports you are not purporting to
22 summarize the entire blockchain ledger?

23 A (JS) Yes. I think that that's accurate. What
24 we summarize is in relation to the activity that
25 we see within what one could call the controlled

1 ecosystem.

2 THE COMMISSIONER: I'm sorry, I missed that last
3 phrase.

4 THE WITNESS: Within the controlled ecosystem.

5 THE COMMISSIONER: Thank you.

6 MS. ROSE:

7 Q And as you said, the controlled ecosystem you're
8 referring to is entities like exchanges and
9 would that also include bitcoin ATMs?

10 A (JS) It would include ATMs. We prefer to call
11 them kiosks because in functionality, you know,
12 ATMs actually have additional controls in place
13 that sync and link to bank accounts, right,
14 whereas these kiosks do not, so it is an
15 important distinction I would make.

16 MS. ROSE: Thank you for clarifying.

17 Mr. Commissioner, could we have "The 2020
18 Geography of Cryptocurrency Report" be marked as
19 the next exhibit.

20 THE COMMISSIONER: 258.

21 THE REGISTRAR: Exhibit 258.

22 **EXHIBIT 258: Chainalysis - The 2020 Geography**
23 **of Cryptocurrency Report - September 2020**

24 MS. ROSE: Thank you, Madam Registrar. I'm done with
25 that document on the screen now.

1 Q Mr. Spiro, could you tell the Commissioner about
2 Chainalysis's professional services team?

3 A (JS) Yes. So Chainalysis also provides
4 investigative support directly. We have a
5 professional services team which is a team of
6 investigators from a diverse array of
7 backgrounds. Some of them are former government
8 investigators, some of them are investigators
9 that have just been within the cryptocurrency
10 space for a long time so they have deep subject
11 matter expertise and knowledge. And this team
12 can be utilized by our clients for specific
13 investigative support on a case-by-case basis.

14 Q We heard evidence yesterday from our RCMP panel
15 members that the RCMP and other law enforcement
16 members are trained to use the Chainalysis
17 software and other software providers by
18 themselves. Could you elaborate on what skills
19 or experience the Chainalysis professional
20 services team have that differs from what law
21 enforcement might have.

22 A (JS) I think the primary differentiator right
23 now would just be the experience that they have
24 in relation to investigative, so the deep
25 investigative experience that they have. We

1 have built out a robust training program and it
2 is in I think everyone's best interest that we
3 make the users themselves become what we would
4 call power users. We've seen the best successes
5 in growth as investigators themselves become
6 savvy and capable with the products. But in
7 some cases either because they are extremely
8 complex or if there's a very tight turnaround
9 and there's a lack of resources for the
10 investigators that are involved in their
11 abilities to execute the investigation in the
12 timetable or time frame that they need to, they
13 could employ our professional services team to
14 support.

15 Q And, Mr. Spiro, is it fair to say that you
16 yourself do not actively provide these on the
17 ground expert level investigation services as a
18 member of the professional services team?

19 A (JS) it is fair to say that I'm not a member of
20 the professional services team. I, in a former
21 life, was an analyst and investigator, but
22 these days that is not my remit.

23 Q But nonetheless could you speak to when it might
24 be appropriate for law enforcement to engage or,
25 you know, not limiting it to law enforcement but

1 also the private sector where it might be
2 appropriate to engage the professional services
3 team.

4 A (JS) Sure. I think one of the issues that we
5 have potentially with the cryptocurrency
6 ecosystem more broadly is you have frictionless
7 payments, right, and the speed and velocity with
8 which these transactions can occur is very
9 different than in traditional financial
10 services. So sometimes when we speak about
11 urgency, right, in relation to things like a
12 hack or theft or other kinds of illicit
13 activity, law enforcement might need to act
14 urgently and quickly to be able to recoup those
15 funds, to freeze those funds, et cetera, wherein
16 they might utilize our professional services
17 team to assist them in doing that within the
18 proposed time frame.

19 Q And turning now to the Chainalysis Reactor
20 software that you previously described, could
21 you speak to the type of proficiency needed to
22 operate that software?

23 A (JS) Yes, so I would say that the software is
24 fairly user friendly. Those that are
25 investigators we have found are able to become

1 proficient with our software. We do provide
2 training that comes with the procurement and
3 usage of Reactor software so we do provide that
4 as well initially. I mentioned that we also
5 have a more substantial training program that
6 can be utilized if investigators want to
7 continue to enhance their capabilities. But it
8 is something that you know, we have seen by and
9 large success from the investigators in law
10 enforcement that we work with.

11 Q But nonetheless it does require some skill
12 building or some knowledge in order to use the
13 software. It's not quite so user friendly as
14 something like a Google search engine?

15 A (JS) That is correct. Yes. It requires some
16 training. I would say for certain.

17 Q And users would need to be able to direct their
18 tracing or direct their searches within the
19 software. The software will not direct them
20 exactly where to go; they will need to exercise
21 a certain level of judgment in how to proceed?

22 A (JS) Yes. So to be clear, we provide data,
23 right, and we provide the information. But it
24 is up to the users to then effectively conduct
25 these investigations and make their own

1 determinations.

2 Q Okay. I think that now might be an appropriate
3 time for us to proceed to the demonstration
4 portion of the hearing today and that will be
5 conducted predominantly by Mr. Place. I'll just
6 check to make sure that our hearing team is
7 ready to go ahead with that and then I
8 understand that the direction is for Mr. Place
9 to share his screen, but please correct me if
10 I'm wrong.

11 SUPPORT TECHNICIAN: We are ready.

12 MS. ROSE: Great.

13 Q Mr. Place if you could proceed. Thank you?

14 A (IP) Sure. Absolutely. Give me just one
15 moment. All right. Can everyone see my screen
16 okay?

17 Q Yes?

18 A (IP) Okay. Great. So again today I'm going to
19 walk through our three core products, the first
20 being Kryptos, which is really our benchmarking
21 and profiling product for the different
22 cryptocurrency businesses within the space. I
23 will then walk through KYT, or Know Your
24 Transaction, which is our transaction monitoring
25 solution providing realtime alerts and other

1 restoring attributions. And then finally I'll
2 walk through Reactor, which is again is our
3 graphing, mapping and investigative tool to
4 follow the flow of funds visually and for
5 certain situations to perform enhanced due
6 diligence.

7 And so this first screen we are looking at
8 here is Kryptos and so when you log into Kryptos
9 you get this initial view where if you want to
10 search by a given service you can type in the
11 name here. When you see categories, essentially
12 again what we do here at Chainalysis is that all
13 of the alphanumeric strings and information on
14 the public blockchain and on the ledger we tie
15 those addresses to real world entities and
16 services and those entities and services
17 ultimately fall under different categories. So,
18 for instance, if I look at our different
19 categories that includes things such as hosted
20 wallets, mining pools, exchanges, scams, stolen
21 funds, these are the sort of types of categories
22 that we are able to identify, services in which
23 they fall under. And --

24 Q Mr. Place, sorry, just if I could interrupt you
25 for just a moment.

1 A (IP) Sure.

2 Q You are going to walk us through this software
3 but are you involved in determining which
4 entities fall within these categories?

5 A (IP) I am not. We have a data operations team
6 that handles that.

7 Q Okay. Thank you. Could you please continue
8 telling us about the Kryptos software.

9 A (IP) Sure, absolutely. So, again, what you are
10 able to do is you are able to create your own
11 custom watch list where if there's maybe a
12 particular set of businesses that you would like
13 to monitor or benchmark or profile you can add
14 them to a custom watch list. Below that we also
15 have all the top 50 exchanges by volume. You
16 can sort by the different risk categories. We
17 can look at their country of headquarters. We
18 can look at some of the different fiat pairs
19 they have within their platform. But what's
20 really helpful is -- for example, I'm click on
21 Gemini. We can see a really robust profile for
22 the respective businesses, and so again, to sort
23 of add or remove things from that watch list we
24 have an easy feature here. But what's really
25 helpful is this information on the left-hand

1 side. Again, this is going to be a Chainalysis
2 risk rating.

3 Q And, Mr. Place, are you -- sorry again. Are you
4 involved in categorizing these entities as being
5 low or high risk? Are you involved in
6 populating the risk ratings that we see on the
7 left-hand side of the screen here?

8 A (IP) I am not. Sorry, go ahead, Jesse.

9 (JS) I can field that question, Kelsey. So
10 I am involved in how we have developed our risk
11 rating. Essentially we have taken a number of
12 indicators coupled with specifics that have come
13 from data, for example, in relation to the red
14 flags and typologies and we've coupled that
15 information in relation to how we score risk, if
16 you will, in relation to entity.

17 Q Right. But, Mr. Place, that's not your area of
18 expertise, is it?

19 A (IP) Correct. I don't work in the risk ratings
20 of the different profiles and services within
21 Kryptos.

22 Q Thank you.

23 A (IP) No problem.

24 Q Please continue.

25 A (IP) Sure. No problem. So, again, below that

1 we have some information including the legal
2 names. We have some headquarters information.
3 We have the country of incorporation, place of
4 incorporation, again the fiat pairs. We also
5 see all the different assets that are traded or
6 accepted on the platform. If you want to expand
7 that list you can easily to do so there. And
8 then additionally we see if there's any stable
9 coins offered, privacy coins and rating fares.
10 We additionally also have information on the
11 most recent news associated to these given
12 platforms or potential negative news or adverse
13 media or just general information about the
14 business in the space. Below that we have
15 alerting functionality which you can see sort of
16 the conditions for which that is set over here,
17 so, for instance, we can see that on the week of
18 September 20 to October 5th there was increased
19 exposures to high risk exchanges and some other
20 categories. If you'd like to further drill down
21 to the specific transactions that led to those
22 spikes in activity you can very easily click on
23 here and identify the specific transactions.

24 What is really helpful as well is we are
25 able to then also identify the varying volumes

1 of transactions to the different categories and
2 services that the business interacts with. So,
3 for instance, you can look at all the different
4 types of activity. You can look at the
5 non-risky activity; look at the risky activity.
6 You have custom date ranges which you can select
7 if you want a particular date range you'd like
8 to examine. But again, just a really helpful
9 way to identify any spikes in activities. So,
10 for instance, on the week of March 9th to
11 March 15th there was over \$466 million being
12 transferred between exchanges and then, you
13 know, some other categories that we also have
14 identified there.

15 Additionally we can benchmark this service
16 against other services and see kind of where
17 everyone stands within, you know, relative to
18 one another. So, for instance, when we're
19 looking at the different volumes we can see for
20 instance that, you know, comparing the week of
21 March 2nd to March 8th this platform was well
22 below the volumes of the top 50 exchanges in
23 some of the high risk exchanges. Below that we
24 also have the top counterparties for this
25 particular service so, we can see for instance

1 Coinbase and OKEx and Bitstamp were some of the
2 largest counterparties to this particular
3 platform that we are looking at for an example.
4 Below that we can also see the total number of
5 counterparties. And so, for instance, we can
6 see a spike here on the week of November 16th,
7 so just recently, a total of 6,891
8 counterparties, and again, if you want to change
9 by the different assets you can click here and
10 view those accordingly.

11 So for the most part -- also click on the
12 alerts tab to show this functionality. This is
13 going to be sort of a comprehensive list of all
14 of the different services you've added to your
15 watch list and all the respective alerts that
16 they've generated. If you want to filter by
17 particular alert types or by particular
18 categories from which those alerts generate, you
19 can do so easily here. And for the most
20 part that's kind of Kryptos in a nutshell, and I
21 think that kind of provides a nice sort of level
22 of insight into what this product does and some
23 of the features behind it.

24 Q Well, thank you. Maybe we could -- sorry, did I
25 interrupt you there? Did you --

1 A (IP) No, no, no. Go right ahead.

2 Q I was saying if that's it for Kryptos maybe we
3 could move on to the KYT, Know Your Transaction
4 software.

5 A (IP) Sure. So here within the KYT solution
6 again this is really the heart of our
7 transaction monitoring solution for our clients.
8 What we have here is the initial dashboard view
9 when you log in. So this is a really great
10 organizational snapshot of the activity on the
11 given platform and the transactions being
12 screened. So this is going to provide a lot of
13 sort of macrolevel insights so when we see
14 "alerts overview" these are essentially the
15 transactions that have been flagged for review
16 based on the parameters that you set within our
17 alerts, which I'll be sure to go over in more
18 detail as we walk through alerts. You see this
19 user overview. This is essentially the user
20 risk segments on the profile because essentially
21 the way it worked -- on the platform, excuse me.
22 The way it works is that ultimately
23 transactions, you know, an individual client on
24 a platform may have more than one transaction.
25 We can then based on those different

1 transactions assign a risk score based on their
2 overall activity. So if you want to drill down
3 to the specific subset of users from here you
4 can do so easily there. Additionally we see
5 information on the latest alerts generated, the
6 different categories from which they were
7 generated, the amounts of which those
8 transactions occurred. And then to the right of
9 that we have again that transfer volume per
10 category chart, and for this example I just
11 selected just the risky activity and what we can
12 do is, for instance, see that on the week of
13 August 10th to August 16th there was a large
14 spike in gambling activity, about \$1.6 million.
15 If you want to look at both received and sent
16 transactions you can do so easily there. And
17 just to clarify, a received transaction is a
18 deposit to a platform and a sent transaction is
19 a withdrawal from a platform. So currently we
20 are looking at both deposits and withdrawals to
21 get this sort of figure, but again, you can
22 select by either-or accordingly or potentially
23 respective category of interest.

24 Q Just to interrupt briefly, Mr. Spiro, and sorry
25 Mr. Place if you could just scroll up slightly.

1 A (IP) Sure.

2 Q Thank you. Mr. Spiro, under the latest alerts
3 on the left-hand side we see that there's
4 darknet market flags. Could you perhaps
5 describe what type of activity would lead to
6 that type of a flag?

7 A (JS) If I understand the question, you mean in
8 relation to the connection to darknet markets,
9 you're not asking about darknet markets and the
10 kind of activity they support themselves. Is
11 that correct?

12 Q I'm just only asking what would lead would lead
13 to this type of flag in this KYT software?

14 A (JS) We've been able to identify transactions in
15 and out of darknet markets. Darknet markets are
16 inherently high risk because of the kind of
17 activity that they support. So identifying that
18 kind of exposure and interaction with a darknet
19 market would lead to these kinds of alerts.

20 Q So would it be fair to say that this flag would
21 not necessarily mean that, you know, someone had
22 purchased Fentanyl, it would simply mean that a
23 purchase was made in a darknet market?

24 A (JS) Yes, there was some kind of transaction
25 associated with the darknet markets. Darknet

1 markets aren't only connected to illicit
2 narcotics. They have a number of different
3 kinds of products and services that are provided
4 on them.

5 Q Thank you. Sorry for interrupting there,
6 Mr. Place. If could you please continue to
7 describe the rest of the software.

8 A (IP) No, absolutely. What I'll do that I think
9 will provide some more context is that I can
10 show the different parameters for which we set
11 this and how these alerts are generated. I
12 think that will help provide some additional
13 context as well. But below that we have an
14 exposure wheel and this particular data visual
15 is very common throughout our products. You'll
16 also see this as we walk through Reactor. And
17 the way it works is that you'll this outer ring.
18 That's going to represent the direct exposures
19 to various services that fall under those
20 perspective categories, and what that means is
21 that it is a direct counterparty in a
22 transaction. So if we, for instance, look at
23 the direct receiving exposure from exchanges
24 then we see that the majority of that is coming
25 from Coinbase, that means that Coinbase is a

1 direct counterparty sending to this platform
2 that we're looking at this example data for.
3 And so when we look at on the contrary the inner
4 ring -- so, for instance, let's look at the
5 inner ring of indirect sending exposure to
6 gambling, what this means is that funds are
7 going indirectly from the platform to
8 intermediary addresses, to an intermediary
9 address or numerous intermediary addresses
10 before reaching that next known service, and the
11 reason that occurs is that a very sort of common
12 and inherent aspect of the cryptocurrency space
13 is the idea of a personal onposted wall. So a
14 wall that is not hosted by a platform, you
15 yourself have the private keys and you are
16 managing the funds yourself. And so when funds
17 are being sent to or from there they're not
18 coming directly from a service and subsequently
19 they will then have what we call indirect
20 exposure. And indirect exposure is definitely
21 an important concept that I'll walk through
22 within Reactor to kind of show you what that
23 looks like and how that can kind of be examined,
24 because really the key point with indirect
25 exposure that we are trying to identify

1 potential change of ownership or to see if there
2 was someone else who may have come across those
3 funds or if the person in question is in fact
4 the one who conducted those transactions
5 indirectly. Below that we have a topic named
6 counterparties which again is just kind of
7 showing you who you are transacting with the
8 most. So you want to sort by the total number
9 of transactions, total number of deposits, some
10 of these other parameters us you can do so here
11 and -- sorry, go ahead.

12 Q Sorry, I want to understand that when you say
13 they are counterpart to a transaction can you --
14 and I'm not sure if this is a question for
15 Mr. Spiro, so please jump in, Mr. Spiro, if it's
16 for you, but could you describe what you mean by
17 being a counterpart [sic] to a transaction and
18 is that something that's being recorded from the
19 blockchain ledger or what does that mean?

20 A (IP) So essentially what this is saying is that
21 this platform is a counterparty. So, like, what
22 we are looking at within KYT we are assuming --
23 we will just assume we're a fake platform. So
24 this is platform X exchange X. And --

25 Q It would be typically used by private sector

1 entities to review the transactions of their
2 clients on their own exchange?

3 A (IP) Correct. And so what we are looking at
4 essentially is saying which other platform has
5 been sending us funds or which other platform
6 have we been sending funds to, and those can be
7 both direct counterparties and indirect
8 counterparties. So right now we are looking at
9 both direct and indirect counterparties. But if
10 I want to say sort by just the direct
11 counterparties, I could click direct only and
12 now I'll look at the results for people that we
13 are interacting with directly. Does that help
14 clarify?

15 Q It does. And so basically if I'm understanding
16 this correctly, and you know, I'm going to put
17 it to you and please if there's anything that
18 I've captured incorrectly please let me know.
19 But basically this is if you have a client on an
20 exchange and they are depositing bitcoin or
21 another virtual asset in their account within
22 the exchange or they are receiving money from
23 outside the exchange, it's being deposited into
24 their exchange account, and then this would be
25 shown in the counterparties here, it would be

1 showing where those transactions originate?

2 A (IP) Correct. Yeah, these are for external
3 sources of funds. So it there is a
4 cryptocurrency deposit, so someone is funding
5 their account with cryptocurrency, not from that
6 platform, that would be like an external
7 deposit. And then on the contrary, if someone
8 is sending funds elsewhere that would be a
9 withdrawal that they are sending funds
10 externally from that platform to another
11 platform.

12 Q Would this be limited to virtual asset
13 transactions or would it also include fiat
14 transactions?

15 A (IP) This is just virtual asset transactions.

16 Q Thank you.

17 A (IP) Sure. And so what I'll do is I'll quickly
18 touch on users and transfers. Alerts is
19 probably the most exciting piece of this all
20 where really sort of the core functionality
21 within this solution lives, but I'll quickly
22 touch on users and transfers. And so what
23 you're able to do is here is in the users
24 tab you can again sort by the different risk
25 scores. So maybe I want to look at just my high

1 risk users. Let's say opened or closed cases
2 because we do have some case management
3 functionality in here for our clients to better
4 work and handle the different alerts and
5 information that they receive from us. So, for
6 instance, if I wanted to say look at all my high
7 risk clients with open or active cases I could
8 simply sort of segment those users here. If I'd
9 like to export this information to CSB and work
10 elsewhere I would be able to do so easily.

11 Then when we look at the transfers view it's
12 actually kind of similar in that again we can
13 filter by particular date ranges. Maybe there's
14 like an audit for a business or they're getting
15 requested transactions over a given date range,
16 they can kind of easily sort that here. Again
17 if they want to filter by the different
18 categories and then the different services
19 within those categories they can also do so
20 there. And what you do see here is with some of
21 these transactions there is a little indicator
22 saying that this transaction did have an alert
23 associated to it, and so for instance here we
24 can see that this particular transaction
25 generated a high risk alert because there's more

1 A (IP) Exactly. Yeah, this allows them. And as
2 we were talking about the concept of direct and
3 indirect exposure, you'll have the ability to
4 adjust the parameters for both of that and then
5 subsequently assign the severity that you
6 believe those different conditions align with.
7 Then you can change the dollar amount as well.
8 So really entire customization of these alerts
9 and how you are able to sort of configure and
10 align them to your respective risk appetite and
11 regulatory requirements.

12 Q And so you know, an exchange could in theory
13 hypothetically be operating in a situation in
14 which they have no concerns about darknet
15 transactions, for example, and they might see
16 that there is an alert in the software but they
17 can be free to disregard it if they so choose?

18 A (IP) Correct.

19 Q And, sorry, I see Mr. Spiro is trying to chime
20 in here. Mr. Spiro, perhaps I direct that
21 question to you.

22 A (JS) Yes, so hypothetically that is something
23 that could happen. But what I would posit and
24 add is that if an exchange were using this
25 product, for example, we would probably be

1 acting under the guise that they fell under
2 regulation to be doing so. And so if they are
3 regulated, right, and if they have are under
4 regulatory supervision, if they are going to
5 dismiss alerts, right, and it is within their
6 risk appetite depending upon the organization.
7 If they were to do that they need to be able to
8 justify to the regulators based on an
9 examination or audit why they made that
10 determination and why they dismissed those
11 alerts versus escalating them.

12 Q Right but they don't need to make that
13 justification to Chainalysis. They would need
14 to make that with the regulator?

15 A (JS) Yes, correct.

16 Q Thank you.

17 A (IP) Sure. I was going to say one minor
18 distinction that is important, too, is that
19 again with direct exposure we know definitively
20 that that's the counterparty, so at that point
21 we know that is clear-cut, we know that is
22 definitely who they received or sent from. But
23 with indirect, that is where often times you
24 might need to go into Reactor and determine if
25 there was a change of ownership along those

1 indirect flow of funds and I've a particular
2 example I'll show that's a real world scenario
3 of a client who received an alert or indirect
4 exposure to something illicit. I'll kind of
5 walk you through how they are able to make that
6 assessment to determine if the person on their
7 platform is in fact the one to conduct a bad
8 activity after they move the funds. And so I'll
9 be sure to walk through that and help provide
10 some more clarity on kind of what that looks
11 like as well.

12 And so again to your point.

13 Q We'll turn it back over to you, Mr. Place.

14 A (IP) Sure. So for the most part, again, like
15 when you go back to the alerts view, I want to
16 look at these respective alerts, I can click on
17 them here. This is a randomly -- this is like
18 an anonymized user ID. This is just so that our
19 clients are able to pair client on their
20 platform to users in our system. This is
21 something that we have a lot of people --

22 Q Sorry. Mr. Place, I'm having a little bit of
23 difficulty seeing. I am not sure if others are
24 experiencing the same thing, but I was wondering
25 if you could zoom in a little bit.

1 functionality where it's very easy to go into a
2 profile. You can tick the transaction if
3 there's an alert on. You can open that in
4 Reactor and begin your graphing and
5 investigative piece there.

6 And so now that we've kind of touched on KYT
7 a bit I'll now move into Reactor and show you a
8 real world example on how this was employed.

9 Q And just to remind -- just to be clear, the
10 Reactor software is where you can actually trace
11 virtual asset transactions?

12 A (IP) Correct. Yep, this is our visualization
13 tool that's going to help you follow those flow
14 of funds and visually identify that. And so --

15 Q And so is this -- oh, so sorry. Is this the
16 tool that would be predominantly used by law
17 enforcement as compared to the KYT which would
18 be predominantly used by private virtual asset
19 service providers?

20 A (IP) Yeah, that's absolutely correct.

21 Q Thank you.

22 A (IP) Yeah, no problem. Sorry for cutting you
23 off there.

24 Q Not at all.

25 A (IP) Great. So when we come into the Reactor

1 product I already have an example graph pulled
2 up, but there's a way where you can have all of
3 your graphs and work that you've been collecting
4 in this My Graph section, but the way it works
5 is that again you can either copy and paste and
6 address or transaction directly into the search
7 bar or directly on to the graph and that
8 information will paste accordingly. But to kind
9 of provide some more context and rather than
10 starting from scratch I think it's helpful to
11 show a real world example. So this right here,
12 this hexagon that you see, this is one of our
13 clients and this is their platform that uses
14 KYT. And they essentially received an alert
15 saying you have indirect sending exposure to
16 sanctions, and so --

17 Q Mr. Place, again I'm sorry to interrupt. I'm
18 again having a feeling that I need to pull out
19 my glasses. So I was just wondering if you
20 could zoom in a bit.

21 A (IP) Yeah. Is that any better? Is that better?

22 Q It's a little better. Yeah.

23 A I don't know if I can zoom in much more than
24 that because it gets a little skewed. But is
25 that okay?

1 Q I think that's okay for now, but thank you.

2 That's much improved, yes. Thank you.

3 A (IP) Yeah, yeah, no problem. Sorry about that.

4 So again, what we're looking at here is a real

5 world example where a client of ours received an

6 alert saying you have indirect sending exposure

7 to sanctions and so what's interesting here is

8 that again this is the concept of indirect

9 exposure. So just for purpose of example let's

10 say that the platform was this one that I've

11 labelled "case 1" and they sent out to the

12 sanctioned entity, that would be direct

13 exposure. This is the direct counterparty of

14 this cluster. And when I use the word

15 "cluster" -- sorry, go ahead, Kelsey.

16 Q Sorry, I'm just wondering you use the word

17 "sanctioned entity." What does that mean? And

18 perhaps, again, if this is a question for

19 Mr. Spiro perhaps he can jump in.

20 A (JS) I can. Thank you. So when we're

21 referencing sanctioned entity it doesn't mean no

22 cryptocurrency wallet itself is sanctioned.

23 However, there are cryptocurrency wallet

24 addresses that have been included in a number of

25 sanctions designations. So as it pertains to

1 sanctions that's how it is flagged and
2 identified. But there are not sanctions on the
3 wallet itself. However --

4 Q And when -- sorry, please continue.

5 A (JS) Interaction with that with those wallets
6 potentially triggers reporting requirements and
7 identification to the Office of Foreign Asset
8 Control in the United States.

9 Q And you said that there are sanctions lists that
10 are prepared or designated. Is that designation
11 performed by Chainalysis or where does that --
12 who prepares that sanctions list?

13 A (JS) The office of [connection disruption] --
14 which is part of the US Department of Treasury
15 produces the sanction sets, what's known as
16 sanctions packages for a number of different
17 kinds of current sanctions that exist in the US.
18 As it pertains to virtual assets you've seen
19 sanctions applied in relation to cybercrime,
20 what's known as the cyber IO designations.
21 You've also seen them applied in relation to
22 what's known as kingpin designations connected
23 to illicit narcotic activity as well.

24 Q Sorry, I'm not sure if it was just me, but it
25 cut out the very start of your answer there. I

1 was just wondering the name of the office within
2 the US Treasury Department is what?

3 A (JS) The Office of Foreign Asset Control, known
4 as OFAC.

5 Q Thank you. Mr. Place, back to you.

6 A (IP) sure. Sorry about any misconception there
7 or apologies for that. So again, essentially
8 this is a client who received an alert for
9 indirect sending exposure to this wallet in
10 question, and so what's really great, though, is
11 that this tool will enable them or investigators
12 to make the determination is the person who sent
13 from here to here the same person that sent from
14 here to the illicit activity in question. And
15 so there's kind of a few ways that we can make
16 that assessment quickly and that we can kind of
17 feel confident in the conclusion we are coming
18 to. And so the first is we can look at the
19 actual timing of the transactions, and so for
20 instance, this transaction, the first one was
21 facilitated on the January 21st at 8:30 a.m. and
22 you see these external sources that I've pulled
23 up here because the reason why I did is
24 essentially we can see that the funds from the
25 platform were sent here and then a larger amount

1 was sent on to the illicit activity. What we
2 can do is we can then take a look at some of the
3 other external funding sources to get a better
4 picture of the activity in question. And so
5 when we start to look at the time of the
6 transactions to again 11:04 a.m. the same day,
7 12:19 the same day, 12:19, 9:30 a.m., 10:30 a.m.
8 and 12:19 p.m. we then look at the amount of the
9 transactions heading up to this 1.97. We can
10 also look at this transaction here and see that
11 this occurred at 12:44 p.m. So all of this
12 activity prior to happened before this
13 transaction was sent on, so to me it's pretty
14 clear that it indicates there was a
15 consolidation of funds from numerous different
16 platforms and services to which they wanted to
17 sort of consolidate these funds and then move
18 them on to this address in question.

19 And what's really great, though, is that the
20 kind of next piece in determining this is that
21 so we see the amounts adding up to the same. We
22 see the times indicating that the funds were
23 consolidated and then moved on. What we'll then
24 want to do is click on this cluster. I should
25 just kind of clarify what I mean by cluster is

1 meaning that this is someone's wallet or wallets
2 that are not on a given platform. It's maybe on
3 their thumb drive. It's on their cellphone.
4 It's on their desktop. It's a wallet that they
5 own the private keys for and it's not a platform
6 or a service that holds those funds. And when
7 you take that into consideration that pretty
8 definitively means for us that it's very likely
9 that this person here also operates this wallet
10 and so when we take in all the factors of the
11 timing of the transactions, the amounts in which
12 it adds up to and that the intermediary is very
13 likely to be a personal unhosted wallet, you can
14 feel quite confident in saying that the person
15 who sent from here to here is in fact the same
16 person who sent from here to the OFAC designated
17 national. So that's kind of in a nutshell how
18 this product can be used to identify potential
19 changes of ownership or non-potential changes of
20 ownership within transactions and again really
21 helpful when we're talking about indirect
22 exposures. Do you have any questions for me on
23 what you are seeing here?

24 Q Yeah, I just wonder if you could build on these
25 little nodes and connections and just describe

1 for us, you know, for example the blue lines
2 that are emanating between two nodes, can you
3 explain to me what those represent.

4 A (IP) Sure. So this intermediary address right
5 here what I was able to do is I go here to the
6 counterparties tab and we're adding in the
7 different funding sources for which this wallet
8 had received funds. So I added the ones of most
9 interest and I can add the other additional two
10 here. And so now we're looking at every
11 potential funding source for this wallet. So
12 again, like when we see these lines it's just me
13 highlighting them, but you can again see all of
14 the different activity coming in and out of this
15 cluster in question. So again, this cluster is
16 made up of seven addresses or you can think of
17 it as different wallets and we are able to again
18 look at all of the differential funding sources
19 from those.

20 So some of those are again going to be more
21 personal unhosted wallets. Some of them are
22 services like the platform that's a client of
23 ours. And then additionally we see, like, a
24 scam. So you'll see a lot of different funding
25 sources. And what I would mention is that this

1 kind of concept of sending to personal unhosted
2 wallets and then to illicit or risky services is
3 kind of like a very common but easy to identify
4 obfuscation technique where in the sense that
5 bad actors and others are potentially aware that
6 you shouldn't be -- some of the sort of ins and
7 outs of what's advantageous for them or not and
8 because of this it's definitely something where,
9 you know, you can really kind of easily identify
10 this and even if there was additional layers of
11 obfuscation you can continue to map that out and
12 identify that with this particular product.

13 Q When you say "funding sources," is this all
14 information that is being recorded in the
15 virtual assets blockchain?

16 A (IP) Yes. These are all transactions on the
17 public blockchain.

18 Q And so is it fair to say that these transactions
19 do not involve -- these transactions all involve
20 coins that have a public ledger like bitcoin?

21 A (IP) Correct. And one thing I should mention is
22 this graph is just for bitcoin. We don't
23 currently have the ability to look at multiple
24 tokens within one graph. So right now you can
25 see up here as notated by the BTC icon we are

1 just looking at bitcoin transactions.

2 Q And could you explain to me. I understand that
3 Chainalysis Reactor software is intended to
4 essentially make the blockchain ledgers user
5 friendly such that you don't require a good deal
6 of sophistication to be able to read the actual
7 blockchain itself, that, you know, the average
8 user can understand what they are looking at.
9 And I wonder how could -- would it be possible
10 for a user to review these transactions without
11 the Chainalysis software if they had the
12 requisite sophistication to review the
13 blockchain ledger themselves?

14 A (IP) No, because the key here -- sorry. Go
15 ahead Jesse.

16 (JS) So essentially there are open source
17 kinds of software like a block explorer that an
18 individual could try and use to conduct an
19 investigation, but due to the complexities, you
20 know, you have this series of alphanumeric
21 hashes that encompass a wallet and what you will
22 find consistently is that if you tried to use a
23 block explorer comparatively, the determinations
24 and attributions that you would make, especially
25 in relation to transaction that has a relatively

1 light degree of complexity, meaning multiple
2 transactions occur and then consolidations
3 et cetera, the attributions would not be
4 accurate. You cannot account using an open
5 source block explorer for some of the kinds of
6 activity that occur.

7 (IP) correct.

8 Q If I were wishing to look at -- just let's for
9 example see there's a transaction here with I
10 think it's 14HCPH4. Yes. If I wanted to see
11 just that transaction into this case 1 node,
12 would I be able to view that transaction by
13 itself on the blockchain ledger without the
14 Chainalysis software?

15 A (JS) You could see a single transaction. You
16 might not be able to identify where it had gone
17 in relation to the fact that we actually
18 identified the entities. So what you would see
19 is the transaction from one wallet with that
20 wallet address to another wallet. You wouldn't
21 be able to say that this transaction went to
22 Coinbase or Gemini or Bitfinex, for example.

23 Q Right. And so the added value that's provided
24 by the software here is the sort of
25 interpretation of the data, but the data would

1 be itself available to users?

2 A It is blockchain public data, yes.

3 Q It would just be -- Chainalysis provides the
4 service of, for example, knowing the hashes, if
5 I can use that right, knowing the hashes that
6 are used by Binance or Bitfinex or other
7 services and so they're able to apply that on to
8 this software; is that correct?

9 A (JS) It's slightly more complex but basically,
10 yes. Essentially what Chainalysis provides is
11 an analysis, right, so is intelligence and
12 analysis of the data to provide further
13 intelligence and insight in relation to what
14 you're seeing. Not only does that make it more
15 digestible, but it also assist it's in relation
16 to being able to effectively investigate and
17 identify new potential leads as well, if we're
18 talking about Reactor, for example.

19 Q Okay. I think that's a big help. Thank you for
20 that clarification. And, Mr. Place, is there
21 any further review of these transactions that
22 you think would be assistive in understanding
23 how the Reactor software works?

24 A (IP) No, and the only thing I would just quickly
25 add on top of what Jesse said is exactly right

1 in that, you know, this information is on the
2 public blockchain, but you can't see which
3 entity or service are identified to that. So
4 you can go on the blockchain and you can look at
5 all these transactions respectively, but you
6 wouldn't know what services they're coming to or
7 from directly or indirectly. And so that is
8 really the important component here and what is
9 really valuable in what we do. But if it's okay
10 now would you like me to stop sharing my screen?

11 MS. ROSE: Yes. Subject to any questions the
12 Commissioner may have those are my questions
13 with respect to the Reactor software.

14 THE WITNESS: (IP) Sure.

15 THE COMMISSIONER: Thank you.

16 MS. ROSE: I wonder if now might be an appropriate
17 time to take a quick break, Mr. Commissioner.

18 THE COMMISSIONER: Very well, ten minutes.

19 MS. ROSE: That would be great. Thank you very much.

20 THE REGISTRAR: This hearing is adjourned for a
21 ten-minute recess until 10:41 a.m. Please mute
22 your mic and turn off your video. Thank you.

23 **(WITNESSES STOOD DOWN)**

24 **(PROCEEDINGS ADJOURNED AT 10:31 A.M.)**

25 **(PROCEEDINGS RECONVENED AT 10:40 A.M.)**

1 anonymity enhancing cryptocurrencies, also known
2 as privacy coin, which provide enhanced
3 encryption and privacy features to potentially
4 obfuscate the ability to trace them.

5 Q And I will turn to some of the specifics of
6 that, but for now I'd like to just speak a
7 little bit to the characteristics of virtual
8 assets. So, Mr. Spiro, can you advise whether
9 bitcoin is still the most popular coin and, if
10 so, do you have any views on why that would be?

11 A Yes. So what we've seen is that bitcoin is
12 still by far the most popular cryptocurrency
13 that is currently used within the ecosystem.
14 The main reason for that, honestly, is
15 accessibility. Bitcoin was the first. It is
16 the most widely featured and accepted and
17 exchanged from the global entities within the
18 ecosystem. It is also the one that I think
19 globally there is the most familiarity with.
20 And when it comes to accessibility that's
21 extremely important because it means that while
22 the savvy users can obviously access it, it also
23 means those that are being introduced or are
24 early on in relation to their engagement with
25 the virtual asset ecosystem can also obtain

1 bitcoin most easily and successfully.

2 Q We heard a little about stable coins yesterday.

3 Could you describe what stable coins are and
4 provide an example.

5 A Yes, so stable coins are essentially backed by
6 something else. There's four kinds of stable
7 coins primarily. You have stable coins that are
8 backed directly by fiat currency. You have
9 stable coins that are backed by commodities,
10 something like gold, for example. You have
11 stable coins that are backed by other
12 cryptocurrency and then you have stable coins
13 that are backed by algorithms. The most
14 prominent stable coins that you will find are
15 those that are backed by fiat currency. A good
16 example and the most widely used would be
17 Tether, which is backed by the US dollar. And
18 so that is a good example. They provide more
19 security and are less vulnerable in relation to
20 fluctuation because obviously they are backed,
21 which is why they are called stable coins.

22 Q And we heard a little evidence yesterday about
23 the different types of virtual currency coins
24 and the difference between an open ledger and a
25 closed ledger. Could you tell the Commissioner

1 about what Chainalysis is seeing as risks of a
2 closed ledger or privacy coin?

3 A Well, in relation to close ledgers, I mean what
4 I can say is that public blockchains are what we
5 follow, right, so there is a number of different
6 coins, if you will, that we're able to follow.
7 But for those closed blockchains you're not
8 going to have a visibility into them. So that
9 is not the kind of thing that we would provide
10 services in relation to if somebody were trying
11 to follow that. You have hybrid blockchains,
12 some of them that are developing that we could
13 potentially follow and trace and that we could
14 do, but you have the public and the non-public
15 which is the best distinction to make there.

16 In relation to privacy coins you have a
17 number of different kinds of privacy coins that
18 have different kinds of anonymity enhancing
19 features. Some of them used advanced encryption
20 things like zk-SNARKS, also known as Zero
21 Knowledge Proofs, which are just a kind of
22 extreme encryption technology. You have also a
23 privacy coins that have features that allow
24 essentially for the privacy to be turned off on
25 or to be turned off. This is known as being

1 shielded versus unshielded. There's a number of
2 different privacy coins, as I mentioned. Some
3 of the more popular would be Monero, Zcash or
4 Dash for example.

5 Q And what are the advantages in your view of
6 privacy coins? Or why might a user -- why might
7 a user seek out a privacy coin?

8 A You mean from a licit perspective or an illicit
9 perspective?

10 Q If there's a discrepancy between the two,
11 perhaps you could provide your insights on to
12 both. Why might a licit user and why might an
13 illicit user turn to a privacy coin? In your
14 view, of course.

15 A So a licit user might turn to a privacy coin if
16 they have extreme concerns around their data
17 privacy and data protection, for example. If
18 they don't want any visibility into the activity
19 that they are executing. There is an ethos
20 historically associated with virtual assets
21 where you do have kind of this cyberpunk
22 mentality from some folks where they just want
23 extreme control and privacy around access. I
24 think that's changed markedly from inception,
25 but it is something that does still exist in

1 some places. You also could potentially have
2 the use by individuals that are in certain
3 jurisdictions with authoritarian regimes or, you
4 know, potentially onerous oversight. So I could
5 see that hypothetically. For bad actors they
6 are extremely attractive because again it
7 potentially allows them to move funds across
8 border or domestically and try to avoid
9 detection by law enforcement, by government, by
10 regulators, by those that would be trying to
11 follow the money, as well as the private sector.

12 Q Are there -- could you speak to some particular
13 use cases where someone might legitimately be
14 using privacy coins for the purposes you
15 mentioned?

16 A Can I speak to a legitimate use case. I mean,
17 yes, you know, again, I suppose somebody is
18 concerned with, you know, government oversight,
19 maybe a government has extreme views or policy
20 in place, maybe they are very worried about
21 capital flight. For example, maybe they are
22 putting extreme controls over their citizens and
23 populations. You know, maybe as a result of
24 those things and other kinds of conflicts, you
25 know, maybe their fiat currency is facing

1 extreme devaluation and problems and so they are
2 looking to obtain a different kind of asset to
3 protect their wealth. Hypothetically that is a
4 potential use case, I guess.

5 Q And building on that we've heard virtual
6 currencies' role as both a currency as well as
7 an investment. Could you elaborate on the price
8 volatility of coins like bitcoin and the way in
9 which virtual assets are used as an investment
10 rather than a currency?

11 A Yeah, I mean there is a substantial volatility
12 that is still associated with many of the
13 virtual assets that exist. You know, some of
14 their value initially was derived from the
15 technology behind them and is still derived from
16 the technology and the potential use cases that
17 can be applied with those technologies, like
18 Ethereum and what is known as the ERC-20. But
19 as an investment what we've seen is by and large
20 in relation to growth and valuation that has
21 been pegged to virtual assets being used for
22 investment purposes versus being used for actual
23 procurement and purchasing and, you know, kind
24 of the traditional uses of fiat currency in many
25 forms or fashion. As a result of that there

1 have been over a number of years relatively
2 extreme swings in relation to the pricing that
3 is associated with different virtual assets.

4 Q Are you able to comment on whether one or the
5 other is more predominant in terms of using
6 virtual currencies, is it more frequently used
7 as an asset or is it more frequently used as a
8 currency for procurement? Is that something
9 that you can comment on?

10 A I think based on our market research I think I
11 would be comfortable saying it's more frequently
12 used as an asset.

13 Q Can you speak to challenges in converting a
14 large amount of bitcoin into fiat currency or
15 another virtual currency?

16 A Yes, so it is not as easy as some might think in
17 relation to their ability to conduct such a
18 conversion. Number one, to conduct conversion
19 from fiat into virtual assets or virtual assets
20 into fiat you're probably going to need to use
21 an exchange that provides those kinds of
22 services and the exchange is going to have to
23 have access to banking to do so. So there is
24 that potential issue. When it comes to large
25 volumes because of the potential impact in the

1 movement of large volumes on cryptocurrency in
2 relation to the liquidity in the market and
3 pricing, right, there are usually limits that
4 are set in relation to how much cryptocurrency
5 could be converted at any given time or
6 transferred at any given time. So there are
7 those I would say potential issues in relation
8 to something at scale.

9 Q And in terms of tracing what are the advantages
10 of coins that operate on a blockchain compared
11 to fiat currency?

12 A So one of the things that attracted me most to
13 the virtual asset space when it comes to
14 anti-money laundering is the transparency and
15 the visibility, the traceability and the
16 providence that it provides is really
17 unprecedented. I liken it to the following
18 analogy. If you were to take a dollar into a
19 convenience store and to purchase something,
20 it's going to be very extremely difficult for
21 you to follow every cent associated with that
22 dollar from inception to wherever it goes;
23 right? But in relation to the transaction
24 history as it pertains to virtual assets into
25 the blockchain, you can follow every single

1 piece consistently, and because of that
2 providence and permanence, you know, it can't
3 be -- you know, fraud can't occur in relation to
4 it. The blockchain is secure in that sense.

5 Q Yesterday we heard Sergeant Vickery of the RCMP
6 describe the on-ramp and off-ramp of virtual
7 assets in reference to the point of conversion
8 from fiat to virtual asset in exchanges or
9 virtual currency kiosks. Do you agree with her
10 characterization of these being on-ramps and
11 off-ramps?

12 A I think it a good characterization. I think
13 when it comes to the way in which you would
14 investigate this and the ecosystem, you can
15 think of the on-ramps and off-ramps being these
16 exchanges how somebody can enter and exit the
17 cryptocurrency ecosystem as the choke points.
18 So where they provide those kind of conversion
19 services, think of them as the choke points
20 because those kinds of entities that provide it
21 should be regulated, should have substantial
22 robust know your customer programs in place for
23 individuals to be able to access them. And so
24 from an investigative perspective the reason I
25 call it the choke point is because if you follow

1 the flow of funds using something like
2 Chainalysis and you're able to follow the
3 illicit money to an exchange, what law
4 enforcement should then be able to do is to
5 issue a subpoena to identify the KYC behind that
6 user and to bring about successful prosecution.

7 Q And why do you say that this is the choke point
8 and what role does regulation have at that choke
9 point in your view?

10 A Regulation is essential because if there is not
11 regulation in place on those choke points on
12 those exchanges, the on-ramps and off-ramps,
13 then it potentially means that they do not have
14 effective compliance programs in place because
15 they are not required to have them; right? It
16 means potentially they are not conducting KYC on
17 their users, they do not have transaction
18 monitoring, policies or procedures, training
19 et cetera; right? It means that if the bad
20 actors attempt to utilize them they probably
21 will be able to do so successfully. And
22 following the money when it comes to
23 cryptocurrency we are able to follow it within
24 the ecosystem. If a person then converts into
25 fiat currency, for lack of a better terminology

1 they are then in the wind. We don't have those.
2 Law enforcement may in fact be able to then
3 follow it from there, but for us that is not
4 something that we do.

5 Q And from the work that Chainalysis does, are you
6 able to speak to the role specifically of kiosks
7 in this conversion point and what the risks
8 might be there?

9 A Yes. So when speaking about kiosks, which are
10 also known as ATMs, they are not all equal, and
11 when I say that what I mean is some do have
12 robust compliance around requiring KYC and
13 specific documentation to access them whereas
14 others do not. Bad actors would obviously seek
15 out that do not have those kinds of
16 requirements, for example.

17 And one of the things that is associated
18 with these kiosks traditionally is higher fees
19 than the fees that are associated with more
20 prominent exchanges, for example, those that are
21 probably regulated. So in relation to the use
22 cases for somebody -- there are some I would say
23 potentially use cases where somebody may just
24 want immediate need, immediate access to
25 cryptocurrency where they would be willing to

1 pay that significantly higher fee, but it also
2 is potentially indicative of bad actors who are
3 paying the fee and in exchange not having to
4 provide that PII and identify themselves which
5 could potentially lead to successful prosecution
6 and law enforcement action.

7 Q And PII, what does that refer to?

8 A Personally identifying information. So usually
9 in association with your access to the global
10 financial system, to a financial institution, to
11 a cryptocurrency exchange, you are going to have
12 to confirm that you are who you say you are.
13 That be it with your passport or your national
14 ID or your driver's licence, usually multiple
15 forms of identification, and usually you have to
16 provide that.

17 Q Similar to the know your client or know your
18 customer obligations data collected?

19 A Correct.

20 Q In terms of other risks some have said that
21 cross border virtual asset transactions might
22 pose a risk. Do you have any views on the risks
23 of any cross border virtual asset transactions?

24 A I mean, I think that the digital payment
25 ecosystem, you know, is just radically different

1 to what you've seen in traditional financial
2 service. Again, when we talk about frictionless
3 payments and accessibility it is just very
4 different technology, and with that technology
5 that are substantial benefits. More financial
6 inclusion, again accessibility. The list can go
7 on and on in relation to the benefits. There
8 are always these potential inherent risks that
9 could exist as well in relation to risks around
10 cross border payments. So, you know, it is
11 something to be considered. But I don't think
12 it benefits the technology, the growth or the
13 potential use case to attempt to really silo
14 that kind of activity. I think it's important
15 to have universal umbrella fairly cohesive
16 regulation, in turn which will provide more
17 financial integrity to the space and eliminate
18 some of those concerns.

19 Q Your work with Chainalysis, the PII or the KYC
20 that is currently being collected by exchanges
21 or by kiosks or other actors, the substance of
22 that data, is it sufficient?

23 A So we don't touch KYC. What I can say is, you
24 know, so our visibility would be limited to some
25 extent. We are familiar with what the practices

1 are employed by some of the exchanges. We are
2 just familiar with what their requirements are
3 in relation to KYC or are not. They certainly
4 are not universal. In some jurisdictions they
5 are far more stringent. In other jurisdictions
6 they are far more lax. When it comes to
7 regulation I would say that that is probably the
8 most important component that I see to
9 effectively regulating and mitigating illicit
10 activity in the space, and in general as it
11 pertains to digital payment, you know, I think
12 that that particular component of verifying that
13 individuals are who they say they are and
14 obtaining that information is extremely
15 important.

16 Q So you mentioned a discrepancy between
17 regulation in different jurisdictions. Could
18 you roughly describe the trajectory of
19 regulation of virtual asset service providers
20 from 2013 to date?

21 A Yes. So in 2013 FinCEN was one of the first to
22 regulate the virtual asset space and they
23 applied the Bank Secrecy Act to virtual asset
24 service providers by defining them as money
25 service businesses. The Bank Secrecy Act is the

1 AML CFT laws within the US that pertain to
2 operation for a number of different kinds of
3 financial institutions, including financial
4 institutions and money service businesses. We
5 saw bits and pieces globally from some other
6 regulators. A lot of it was just in relation to
7 guidance or some potential advisories that came
8 out, and then since 2019 we've seen a rather
9 rapid flurry of activity. That was driven by
10 and large by the Financial Action Task Force
11 when they released their virtual asset
12 recommendations. The Financial Action Task
13 Force, also known as FATF, is an [indiscernible]
14 body that has a mandate of building out capacity
15 for AML CFT within the regulatory environment
16 globally. And they do so by releasing
17 recommendations and after releasing
18 recommendations they conduct mutual evaluations
19 where they evaluate the countries that fall
20 under this umbrella that are over 200 in total.
21 You have 39 core members of the Financial Action
22 Task Force and then you have what is known as
23 FSRBs, FATF style regional bodies. In total you
24 have over 200 jurisdictions that fall under that
25 umbrella. And so the mutual evaluations measure

1 how well and how effective the jurisdiction has
2 aligned or implemented those recommendations
3 that have come out. There are no regulatory
4 requirements connected to the Financial Action
5 Task Force, but the results of a poor mutual
6 evaluation are substantial on a jurisdiction.
7 It potentially impacts their access to the
8 global financial system, their credit rating,
9 their ability to obtain lending. There's
10 substantial impact if they receive a poor mutual
11 evaluation and that aligns with them potentially
12 being blacklisted what is known as blacklisted by
13 FATF, which is a very small list, or being
14 greylisted, which is a slightly larger list in
15 relation to the jurisdictions that fall under.

16 So FATF released those virtual asset
17 recommendations in June of 2019 and since then
18 as kind of a benchmark you've seen jurisdictions
19 begin to align with those recommendations, begin
20 to introduce regulation around the virtual asset
21 space. It hasn't been a domino effect, I would
22 say, but it is something where we've seen some
23 progress occur between 2019 to 2020. There was
24 a year review of the progress as a result of the
25 recommendations being released that happened

1 A I was not the author, no.

2 MS. ROSE: Okay. Mr. Commissioner, I'd ask that we
3 have this marked as the next exhibit.

4 THE COMMISSIONER: All right. I think we are at 259,
5 Madam Registrar.

6 THE REGISTRAR: Yes, exhibit 259.

7 **EXHIBIT 259: FATF Report - Virtual Assets Red**
8 **Flag Indicators - September 2020**

9 THE COMMISSIONER: Thank you.

10 MS. ROSE: Thank you.

11 Q In your view -- sorry, Madam Registrar, we don't
12 need to have the document on the screen any
13 longer. Thank you.

14 Mr. Spiro, in your view are these indicators
15 useful?

16 A Yes. I would say these indicators are extremely
17 useful. They were extremely prescriptive, well
18 thought out. I think they will be extremely and
19 are extremely useful for both regulators, for
20 law enforcement and for the private sector as
21 well.

22 Q And we can take it back on the screen if you
23 like, but there's a comment at page 6 about
24 suggesting that the virtual asset exchanges
25 determine if an address has been identified as

1 holding stolen funds or linked to that address.

2 Are you familiar with that requirement?

3 A Yes.

4 MS. ROSE: Sorry, I'm just receiving a message from

5 one of our witnesses. I wonder,

6 Mr. Commissioner, could we take a five-minute

7 break or three-minute break even?

8 THE COMMISSIONER: We'll take five minutes, thank

9 you.

10 THE REGISTRAR: This hearing is stood down for

11 five minutes until 11:14 a.m. Please mute your

12 mic and turn off your video. Thank you.

13 **(WITNESSES STOOD DOWN)**

14 **(PROCEEDINGS ADJOURNED AT 11:09 A.M.)**

15 **(PROCEEDINGS RECONVENED AT 11:15 A.M.)**

16 THE REGISTRAR: This hearing is now resumed.

17 Mr. Commissioner.

18 **JESSE SPIRO, a witness**

19 **for the commission,**

20 **recalled.**

21 MS. ROSE: My apologies for that impromptu break,

22 Mr. Commissioner. We are dealing with some

23 technical issues. I'll resume my examination of

24 Mr. Spiro now.

25

1 **EXAMINATION BY MS. ROSE (continuing):**

2 Q We had just been speaking about the FATF
3 indicators, I believe, and I wanted to ask you,
4 Mr. Spiro, from your experience in working with
5 Chainalysis and tracing virtual asset
6 transactions what in your view do virtual asset
7 service providers and law enforcement need to
8 know about identifying suspicious transactions
9 beyond what is stated in the FATF virtual assets
10 document?

11 A Well, I think in relation to the document it
12 defines potential indicators. Sometimes you
13 will have some of those potential indicators
14 used in conjunction; right? And potentially
15 those indicators themselves are not indicative
16 of illicit activity, like the use of VPN by
17 itself. I think that also in relation to some
18 of the kinds of potential activity that you
19 would see in relation to different kinds of
20 transaction patterns, for example, while it's
21 referenced it may not have been explicitly
22 defined there in some instances. There are
23 other kinds of illicit activity that have not
24 been flagged here, things like extraction
25 attacks which are extremely technical that are

1 indicative of illicit activity as well. But
2 again, I think it was a very measured approach.
3 I think there are a lot of good indicators
4 there. I think they elicited a lot of feedback
5 in relation to the production from many
6 different jurisdictions and I think by and large
7 it's an extremely valuable resource.

8 Q Given your work in certain intergovernmental
9 groups I take it that you are familiar with the
10 some of the regulation of virtual asset service
11 providers in Canada?

12 A That is correct.

13 Q And could you comment on what you see as being
14 the major gaps, if any, in the Canadian and the
15 British Columbia regulation of virtual assets?

16 A I think as a whole, to be fair and transparent
17 I'm not as familiar with British Columbian
18 regulations itself. In relation to Canadian
19 regulation and PCMLTFA, I believe it is, any
20 implementation -- application, I should say, to
21 virtual assets, I think that that is
22 encouraging. I think the fact that it aligns
23 closely with the Financial Action Task Force
24 recommendations is also encouraging in relation
25 to recordkeeping, in relation to the kind of

1 core compliance essentials, you know, having a
2 compliance officer, policies and procedures,
3 training, et cetera. You know, suspicious
4 transaction reporting, all of that kind of
5 activity. So I think that that is a valuable
6 step in the right direction. I will say that
7 one of the potential issues, and this isn't
8 specific just to Canada but many jurisdictions
9 around the globe, is while they are implementing
10 this regulation, defining supervision and having
11 the resources applied to supervision to
12 examination are all things that I think are
13 developing and potentially in flux, and that is
14 potentially the case in Canada as well. You
15 know, I think by and large sans a couple of
16 jurisdictions around the world, this is still a
17 developing place, and I think that that critical
18 component in relation to the actual supervision,
19 having that in place so there is a formal
20 oversight not just the requirements that are
21 applied, not just registration and having the
22 program in place but actually utilizing it
23 effectively, and I'm talking about the private
24 sector right now, requires that oversight from
25 the public sector to do so.

1 Q And first I must commend your mastery of the
2 acronym of the Canadian legislation, the
3 PCMLTFA. You are referring to the Proceeds of
4 Crime (Money Laundering) and Terrorist Financing
5 Act I believe?

6 A Correct.

7 Q And do you have any views, you know, from your
8 experience do you have any views on how the
9 amendment in the PCMLTFA could be improved in
10 future?

11 A You know, I hark to generally one of the things
12 that I like to fixate on, and again, I'm talking
13 more been global regulation but it could be
14 applied here, is what we have seen is the
15 extreme inherent value to what can be done in
16 relation to transaction monitoring. So applying
17 more requirements and specific focus around how
18 that should be conducted and should be done I
19 think is important because it is unique in the
20 virtual asset space as it pertains to what you
21 can see, what you can arrest, you know, the
22 velocity in which you can do that. In virtual
23 assets it can be a proactive response and in
24 traditional financial services it is usually
25 reactive. What I mean by is that an illicit

1 activity will occur successfully; it will be
2 identified after the fact; a red flag, a
3 typology will be identified and they try to
4 arrest it again in the future potentially. But
5 here because you have this capability because
6 you can monitor in realtime and screen
7 transactions in realtime and identify associated
8 risk, I think putting more requirements around
9 that specifically would be extremely beneficial.

10 Q You mentioned earlier in your testimony that
11 there are discrepancies in regulation by
12 different jurisdictions around the world. Why
13 does that matter in your view?

14 A So if you have discrepancies, and you always
15 have slight nuanced discrepancies, so that's
16 important to note, because based on local laws
17 and different potential requirements that they
18 have it's unlikely that you will have directly
19 aligned regulation AML CFT regulations, so there
20 might be slightly nuanced differences. But
21 those for do that apply it at all, have not
22 applied it at all, what you then develop
23 potentially are instances of regulatory
24 arbitrage, right, because if regulation does not
25 exist in a jurisdiction it means that the

1 entities operating in that jurisdiction are not
2 subject to it. It means that they can have more
3 lax compliance or non-existent compliance and
4 what that potentially means is that all of the
5 illicit activity will seek out and go to those
6 places where they can function and execute their
7 transactions successfully.

8 Q Are you -- and by "you" I mean you and
9 Chainalysis -- are you seeing the impact of
10 this? Are you seeing this happen?

11 A What I would say is there been a relative
12 constant in relation to where we've seen a lot
13 of the illicit activity going, but those
14 jurisdictions where we have seen that happening
15 do have more lax regulation, low to no
16 enforcement, so it does align in that sense and
17 that has been relatively constant for a long
18 time. If you go back and look at more legacy
19 information I think you have seen the shift, I
20 certainly think you saw a lot more illicit
21 activity going through the US than you do in the
22 last number of years as FinCEN, for example, has
23 really ramped up their programs. But a lot of
24 it is still going through certain regions.

25 Q And could I ask you to be a little specific on

1 what you are seeing that leads you to the
2 conclusion. Is it that more transactions that
3 have connections to darknet, you know, are
4 originating or ending in a particular
5 jurisdiction that is known to have lax
6 regulation, or can you just describe for me what
7 exactly you are seeing in that regard?

8 A We are actually seeing the majority of all
9 illicit activity, be it connected to ransomware,
10 to scams, to fraud, to darknet markets. We are
11 seeing the majority of it going to a specific
12 region, and a lot of that is going through two
13 very large exchanges themselves that are subject
14 to where they directly exist less regulation and
15 regulatory oversight.

16 Q And are you able to provide the names of those
17 exchanges?

18 A I believe it's referenced in the cryptocrime
19 report, so I would be more comfortable referring
20 to that document.

21 Q Sure. Just excuse me for a moment while I just
22 find the reference.

23 MS. ROSE: Madam Registrar, if we could pull up
24 appendix A which I believe is exhibit 257. If
25 we could have that on the screen. And, Madam

1 Registrar, if wouldn't mind turning to page 9 of
2 that PDF document. Thank you.

3 Q So, Mr. Spiro, does this document assist you in
4 providing the answer to my question?

5 A Yes. I believe the this document says that over
6 50 percent went to two exchanges in relation to
7 illicit bitcoin between 2016 and 2019, which
8 were Binance and Huobi.

9 Q And that statement is listed underneath this
10 colourful graph; is that right?

11 A Yes, that's correct.

12 Q And what would you suggest or what would you see
13 as being necessary on the basis of the work that
14 Chainalysis is doing for improvements in future
15 regulation in terms of where the market is
16 headed? Do you have any recommendations in that
17 regard?

18 A You know, I think regulation is meant to be
19 flexible. I think one of the concerns that I
20 think I share with many others is this is a
21 technology that is advancing so rapidly that the
22 question can be posed will it keep up. Will
23 regulation be able to keep up with the
24 technology as it advances. So I think a
25 vigilance in relation to monitoring different

1 kinds of activity is certainly something that is
2 important, and from a regulatory perspective I
3 think that means providing regular guidance and
4 advisories and updates as different kinds of
5 activity are identified and potential regulatory
6 change if required.

7 MS. ROSE: Madam Registrar, could we turn to page 81
8 of this document.

9 Q Mr. Spiro, would you -- are there any regulatory
10 changes that you see might be appropriate in the
11 future in response to these four developments on
12 where the virtual asset market is going?

13 A I mean, I do see potential changes as it
14 pertains to privacy coins and that is something
15 that was cited by FATF. I think that as with
16 any other instance as it pertains to anonymity
17 and privacy, I think that if law enforcement and
18 governments and regulators can't follow illicit
19 activity successfully then those kinds of
20 entities or services or whatever it might be
21 cannot continue to exist because the potential
22 impact that they have on financial integrity, on
23 things like global terrorism and child
24 exploitation and all kinds of illicit activity,
25 because at the end of the day there's such an

1 interconnectivity with money; right? And so you
2 know, for those kinds of privacy coins that
3 provide full anonymity and are more difficult to
4 follow, track and trace, there will be
5 potentially I think be more regulation that we
6 see adapted by jurisdictions which will point to
7 the fact that if exchanges, if those that are
8 regulated cannot control, cannot identify and
9 cannot follow the flow of funds associated with
10 those kinds of coins, that they then in turn
11 probably will not be able to support them on
12 their platforms and be regulatory compliant.

13 Q So I'd like to turn now to the topic of OTC
14 brokers. Perhaps, Madam Registrar, could you
15 turn to page 13 of this report. And I'll ask
16 you a couple of general questions, Mr. Spiro,
17 before turning to the specifics of the report.
18 Could you describe for us the function of an OTC
19 broker.

20 A Yes. So OTC brokers play a very significant and
21 important part in the cryptocurrency ecosystem.
22 You know, essentially they support liquidity and
23 stability and they provide an avenue for
24 individuals that are looking to buy and sell
25 large amounts of cryptocurrency. They also

1 provide an additional layer of privacy in
2 relation to those transactions, which those
3 investors that are, you know, eliciting large
4 volumes they may desire. So they are an
5 important part of the ecosystem and essentially
6 for a fixed price they allow individuals, the
7 broker, supports individuals buying and selling
8 large amounts of cryptocurrencies. Some of
9 these OTCs are what is known as nested. It's a
10 similar concept to nested banking wherein they
11 provide the service and then the broker
12 themselves has access and an account at a larger
13 entity like an exchange.

14 Q If a user on a particular exchange were to
15 attempt to move a large volume of let's say
16 bitcoin without using an OTC broker what would
17 happen?

18 A So usually as I mentioned before they are going
19 to be transaction limits; right? Potentially
20 that is problematic for them because say there
21 is a transaction limit they can only move a
22 certain amount. Based on what we mentioned
23 previously about the volatility and pricing they
24 may not be able to move that amount with that
25 fixed price that they had associated or wanted

1 to use. Also that kind of movement, you know,
2 OTC transactions are seen as kind of off market.
3 That kind of movement directly from an exchange
4 because of the transparency, the blockchain
5 potentially has an impact on the market also,
6 right, because if people see this kind of
7 massive movement of funds it potentially
8 triggers based on the volatility, you know,
9 rapid change in pricing and, you know, the
10 associated --

11 Q Right. Would it be fair to make an analogy to
12 something on the stockmarket, for example if
13 someone were to purchase a very large amount of
14 a particular stock that that might impact the
15 overall price of the shares that were
16 transferred later on?

17 A Yes. I think that's fair.

18 Q And you mentioned there is an increased privacy
19 associated with OTC brokers. Can you describe
20 how that is the case and what role of collecting
21 KYC information OTC brokers have?

22 A Yes. So on a base level because it's offmarket,
23 right, potentially there is more privacy because
24 it's not connected to directly to individuals on
25 the exchanges in relation to that transaction.

1 But in relation to KYC I think KYC collection
2 and compliance generally that's exercised by OTC
3 brokers varies very widely. You have some that
4 are extremely compliant that have good
5 compliance programs, like Circle, like
6 Cumberland Mining, for example. Those are two
7 good examples. But you are others that utilize
8 and execute very low levels of compliance and
9 may not require any KYC in relation to executing
10 transactions.

11 Q So in referring to this report here we are at
12 page 13 of exhibit 257, which is the
13 Chainalysis -- sorry. No, still at 13. Sorry,
14 Madam Registrar. So this is the Chainalysis
15 cryptocrime report and we are at page 13. This
16 page describes what Chainalysis is referring to
17 as a set of OTC brokers as the Rogue 100. Are
18 you familiar this characterization, Mr. Spiro?

19 A I am.

20 Q Can you explain at a high level how Chainalysis
21 would determine that an OTC broker is likely
22 involved in money laundering?

23 A So we follow the money, right, so it's fairly
24 easy, basically by the flow of funds. If we see
25 substantial illicit financial proceeds going

1 through certain kinds of accounts and based on
2 the kinds of transaction history that we are
3 able to see, we are able to reasonably ascertain
4 the fact that these individuals are actively
5 egregiously, you know, participating in
6 supporting money laundering by way of engaging
7 directly with those that are involved in illicit
8 activity.

9 Q I got a lit bit ahead of myself. Can you just
10 tell us what is the rogue 100?

11 A It is 100 OTC brokers that we've identified that
12 have engaged in substantial volumes of with
13 illicit cryptocurrency and illicit proceeds and
14 have processed transactions and trades with bad
15 actors and wallets that are associated with
16 large volumes of illicit proceeds.

17 Q From your experience with Chainalysis are you
18 able to speak to what features of OTC brokers,
19 and particularly these Rogue 100, might be
20 attractive to a potential money launderer?

21 A There are a few. I mean, when you say -- when
22 you say attractive to a money launderer do you
23 mean for bad actors to seek out specific kinds
24 of OTCs or what features in an OTC might be
25 attractive to a money launderer generally?

1 Q Perhaps I'll ask a couple of other questions as
2 sort of background. Is it your understanding
3 from this report and perhaps other sources that
4 OTC brokers are disproportionately favoured by
5 potential bad actors including money launderers?

6 A Yes, I'd say that's accurate.

7 Q And can you comment on why that's the case?

8 A I think that these OTCs in particular are --
9 have either solicited business in a way that
10 encourages their acceptance of illicit activity
11 or they have been identified because of
12 particular features or attributes that would
13 make them attractive, meaning that they do not
14 conduct KYC, they do have compliance. They are
15 nested within many instances exchanges that also
16 have very low compliance threshold or did have
17 at the time of publish here low thresholds and
18 compliance procedures. I should add that as a
19 caveat this was from 2019, so there is the
20 potential that some of these things have been
21 improved by these entities and others. But if
22 they don't have those kinds of requirements and
23 if they provide access to fiat by way of the
24 nesting service, and if the exchanges that they
25 are using, right, are not conducting customer

1 instances so they would be able to potentially
2 validate if they were using the service like
3 ours. They also might be able to validate it if
4 they were doing appropriate customer due
5 diligence. The thing about these OTCs is
6 usually we are talking about significant
7 volumes, you know, so based on customer due
8 diligence, source of wealth checks, they should
9 be able to identify what business these
10 individuals are in. So there's a number of
11 different potential ways where they would be
12 able to have visibility.

13 Q And are there any particular measures that you
14 are aware of that could be used to improve
15 visibility of these OTC brokers?

16 A I mean, I honestly think that we have fairly
17 good visibility into, as I mentioned, you know,
18 the on-chain activity, the kinds of activity
19 that is occurring, the illicit financial flows
20 that are associated with some. I think the
21 visibility does exist, so I don't think it
22 necessarily needs to be improved. I do think
23 the onus in part falls on additionally the
24 exchanges that are connected to these OTC
25 brokers. Because if the exchanges are compliant

1 and are trying to do compliance successfully
2 they will say to the OTCs if the OTCs try and
3 bring them a significant volume of crypto that
4 is tainted cryptocurrency that they will bar
5 them from their platform, for example. That
6 would be a motivator for the OTCs to act
7 accordingly.

8 Q So is it necessary in your view for a regulator
9 to require KYC directly from the OTC, or is it
10 sufficient as you've described that the exchange
11 which already has in many jurisdictions KYC
12 requirements simply sort of pass on those
13 requirements to clients on its service,
14 including OTC brokers?

15 A I mean, this would be my personal opinion. I'm
16 not speaking on behalf of Chainalysis when I say
17 I think KYC requirements on the OTCs is probably
18 a good idea. Just because, you know, when you
19 are talking about third party, fourth party,
20 fifth party risk that potentially becomes
21 difficult to track and to follow successfully
22 and putting those kinds of requirements on an
23 exchange seems onerous.

24 MS. ROSE: Okay. Madam Registrar, could I turn to
25 page 7 of this document, please.

1 Q So, Mr. Spiro, at number 2 of page 7 here there
2 is a statement by Chainalysis that money
3 laundering is the key to cryptocrime. Could you
4 elaborate on that.

5 A I think when it comes to -- what we are
6 essentially saying is that when illicit activity
7 occurs anywhere, if the bad actors are trying to
8 move it through the cryptocurrency ecosystem,
9 money laundering is the component because we
10 talked about the choke points, right, so what
11 they are trying to do is to successfully
12 obfuscate the flow of funds, the ownership so
13 that they can either enter or exit. And so it's
14 central to the illicit activity that we see in
15 the cryptocurrency space.

16 Q And I understand that through the work that
17 Chainalysis does evaluating trends and such,
18 would you be able to comment on what you are
19 seeing as common typologies of illegal activity
20 and money laundering happening on exchanges or
21 otherwise in the virtual asset space?

22 A I mean, I think we have referenced a number of
23 those common typologies that we just talked
24 about. I will say that I think an interesting
25 distinction and change that we've seen this year

1 from last year is if you look at the 2020
2 cryptocrime report that we provided a lot of the
3 illicit activity in 2019 was associated with
4 scams and fraud, particularly two major scams
5 which were Plus Token and OneCoin, whereas this
6 year what we're seeing is a 600 percent increase
7 in relation to payments associated with
8 ransomware. So just a marked huge change in
9 relation to that kind of associated activity,
10 which I think tracks with probably a lot of what
11 you've seen in the press and heard in relation
12 to ransomware and how it's impacted the globe in
13 the last year. That certainly, I think, could
14 be defined as a trend. We've talked about some
15 of the specific laundering typologies already
16 and I think many of the prominent ones, but that
17 is a trend that we've seen this year that I
18 think is important to note.

19 Q And one of those techniques for money laundering
20 that you described is using a mixer or a
21 tumbler; is that right?

22 A That is correct.

23 Q And in your view that continues to be a
24 predominant typology of money laundering in
25 connection with virtual assets?

1 A We do still see mixers and tumblers used, yes.

2 MS. ROSE: Madam Registrar, could we turn to page 21
3 of this report. Just scroll down a little bit.

4 Q Mr. Spiro, can you describe this picture on the
5 screen here?

6 A Yes. So essentially what you have is you
7 have -- when we talked about tumbler at a high
8 level view it was my explanation where these
9 coins were mixed up and you returned a different
10 output, and this is what it actually looks like
11 in practice where there are algorithms that are
12 used, a myriad of transactions are conducted.
13 These mixing algorithms continue to mix up this
14 cryptocurrency and then there's consolidation
15 that occurs.

16 Q I'll attempt to do some analysis of this and I
17 am hoping you can tell me whether I've correctly
18 assessed it, but my understanding is that a
19 normal transaction you would have point A and
20 point B, point A being at the top left-hand
21 corner of this image and point B being at the
22 bottom right-hand corner of this image. And
23 normally you would see a pretty straight line
24 from A to B?

25 A Correct.

1 Q Is that right? Yeah. And in this pattern you
2 are seeing a number of nodes that are sort of
3 interrupting the chains. You're also seeing
4 that the transaction has been split into a
5 number of different lines here that then flow
6 through these different nodes, but nonetheless
7 eventually the funds do arrive at what's
8 referred to as the consolidation point at the
9 bottom right-hand corner of the screen; is that
10 right?

11 A That's correct.

12 Q And this is a service that is provided by
13 software that's called a mixer or a tumbler?

14 A That is correct.

15 Q And so it makes it more difficult to trace the
16 transaction with a model like this than if it
17 was a straight line from A to B; is that right?

18 A That is correct.

19 MS. ROSE: Okay. And, Madam Registrar, could we
20 please turn to page 22. And, Madam Registrar,
21 could we zoom in on the image here. And maybe
22 scroll up just a little. There. That's great.
23 Thank you very much. Maybe we could scroll up a
24 little bit, Madam Registrar. There.

25 Q So, Mr. Spiro, could you tell me what we are

1 seeing in this image?

2 A Yes. So let's see here. When we're talking
3 about -- I believe what we're talking about here
4 is peel changes, and I had mentioned peel chains
5 before which is where you have a number of
6 wallets that are utilized by the same individual
7 or individuals; right? They are processing a
8 number of different kinds of transactions.
9 Eventually you will have some consolidation
10 point or points in relation to this graph and
11 you have to forgive me because this is not a
12 graph that I'm particularly familiar with, but
13 essentially this is a laundering typology which
14 is connected to a number of kinds of potential
15 resources that would be used by bad actors. So
16 you have peel chains, the use of an OTC, you
17 have mixing service that is used as well and
18 then additional consolidation. So I would
19 define this as a more complex laundering
20 typology that is actually employing different
21 methods.

22 MS. ROSE: Thank you. Madam Registrar, I think that
23 is all I need for this document. Thank you.

24 Q And one OF the other typologies you mentioned,
25 Mr. Spiro, is chain hopping. I know you've

1 spoken approximate it a bit before, but could
2 you just explain briefly what the process of
3 chain hopping is.

4 A Yes. The process of chain hopping is fairly
5 easy to explain, which is that an individual
6 will take a certain kind of cryptocurrency and
7 will convert it to another kind of
8 cryptocurrency and then process a number of
9 transactions in each accordingly, potentially
10 using a number of different kinds of
11 cryptocurrencies. Sometimes they will be doing
12 this utilizing cryptocurrencies like altcoins,
13 which are those coins that have far less
14 liquidity in the market, smaller values. So
15 they do this because, and my colleague had
16 alluded to this previously, it is harder to
17 follow the funds in that way. Potentially
18 visually even, you cannot graph them together.
19 So it is a technique that is used by bad actors
20 sometimes, chain hopping, to try and obfuscate
21 the flow of funds.

22 Q Are you familiar with the recent FinCEN penalty
23 issued to Larry Dean Harmon, who I understand
24 was running Helix and Coin Ninja?

25 A I am.

1 Q Could you describe what services Helix and Coin
2 Ninja were providing?

3 A Yes, they were providing mixing and tumbling
4 services. They were soliciting customers off
5 the darknet. They were providing exactly the
6 kinds of services that we just described.

7 Q And are you familiar with FinCEN's process
8 against those companies?

9 A Yes. There was actually parallel process. I
10 believe there was criminal charges that came
11 from FinCEN as well. But FinCEN had put out the
12 penalty because based on the nature of activity
13 that was associated with these mixers and
14 tumblers that Larry Harmon operated, it was
15 defined as a money service business and was
16 therefore subject to the Bank Secrecy Act and he
17 was in violation, egregious violation, of Bank
18 Secrecy Act on multiple levels. He was not
19 conducting recordkeeping. In fact he was
20 specifically and maliciously deleting any
21 information associated with users. He was not
22 filing suspicious transaction reports, which
23 probably would have encompassed almost every
24 transaction, if not every transaction, that he
25 processed, and there was a mountain of other

1 particulars that were in violation. So he faced
2 this civil penalty.

3 Q And these details of the process that you are
4 describing are public record and publicly
5 available?

6 A Yes.

7 Q Can you speak to -- are there any -- do you see
8 any legitimate uses for tumblers or mixing
9 services?

10 A I mean, any time that we're talking about
11 obfuscation or privacy, again I would just refer
12 to the specific example that I provided before
13 where there are a handful of potential use cases
14 I could say with legitimacy, but I think it's a
15 relatively small scope, to be honest.

16 Q So my understanding is, and I'm happy to take
17 you to a document if you would like, but my
18 understanding is that there is a rather large
19 volume of transactions conducted on Helix and
20 Coin Ninja. Do you know the particulars of the
21 volume of transactions or the dollar value of
22 same?

23 A It was thousands of transactions. I believe it
24 was over \$300 million, I think, estimated in
25 relation to those transaction volumes. So it

1 was substantial.

2 Q And my next question was going to be is this a
3 large volume in the context of virtual asset
4 transactions generally?

5 A It is a significant volume that I'd say. It's a
6 significant volume in relation to illicit
7 activity, yeah. I'd be comfortable saying that.

8 Q And I also understand that you're familiar with
9 the recent US Department of Justice seizure of
10 virtual assets in connection with Silk Road?

11 A That is correct.

12 Q Do you think you could describe for us what that
13 incident involved?

14 A Yes. So Silk Road was the original darknet
15 market that existed for procurement of illicit
16 narcotics and a host of other kinds of services
17 that they provided and products that they
18 provided. The operator Ross Ulbricht, also
19 known as the "Dread Pirate Roberts," was
20 arrested in 2013, the site was shut down, but
21 active and ongoing investigations continued in
22 relation to those that were providing services
23 on the site and the associated illicit financial
24 flows. Chainalysis was used by federal
25 investigators to identify 54 previously unknown

1 transactions that had been associated with Silk
2 Road. One of those transactions by way of an
3 additional transaction was connected to a
4 hacker. And recently the US Department of
5 Justice seized I believe at this point
6 significantly over 1 billion, probably closer to
7 upwards of \$1.5 billion of cryptocurrency in a
8 single wallet, and they did that by utilizing
9 Chainalysis, as I mentioned, to identify
10 additional transactions and connected activity.

11 Q When was the Silk Road operating, roughly?

12 A It operated for a number of years. You'll have
13 to forgive me. I don't know exactly how long it
14 was in operation. I know it was shut down in
15 2013. It was not particularly old. It was
16 operational for a few years. I know that.

17 Q And so can you explain to me, the funds that
18 were seized by the DOJ they were connected to
19 one wallet, you said?

20 A They were connected to one wallet; that is
21 correct.

22 Q And you're able to trace that wallet to activity
23 on the Silk Road?

24 A Yes.

25 Q Is it accurate to say that those funds were

1 sitting in the wallet since 2013?

2 A Almost all of the funds. There were a small
3 number of the funds were exited by way of an
4 additional exchange that has since been shut
5 down known as BTCE, which was a primary vehicle
6 for many years for bad actors looking to move
7 funds.

8 Q Is it -- sorry, please continue.

9 A I was going to say the majority of it, yes.

10 Q Is it common for virtual assets users to park,
11 if I can use that word, their funds in a wallet
12 for that amount of time?

13 A In some instances. It really depends on the
14 particulars, but if it is a very well known what
15 we would consider to be a hot case or activity
16 that's associated with it, because bad actors
17 potentially know that, you know, law enforcement
18 investigators and others will be following the
19 money and attempting to follow the money, it
20 might sit dormant for a few days or a few
21 months, even potentially a number of years. It
22 varies in relation to the activity. But it does
23 occur, yes.

24 Q And can you explain the role of FinCEN and other
25 regulation in enabling the seizure of these

1 funds?

2 A Well, I think this was more driven by law
3 enforcement, and I would like to address that
4 directly in a moment. I think generally what I
5 will say is with regulation and the way in which
6 regulation has continued to develop in relation
7 to AML/CFT requirements in relation to the
8 capabilities of both the private and public
9 sector, as that has continued to develop and as
10 the technologies that support investigations and
11 compliance have continued to develop, it lends
12 itself to more success stories and successful
13 investigations. But I would say tying it into
14 law enforcement, which is important, you know,
15 this year there are a number of prominent cases
16 where Chainalysis has been used and cited
17 publicly in relation to successful be it
18 prosecutions or seizure or civil forfeiture
19 orders. You know, you had this case which was
20 over a billion dollars. There was the Welcome
21 to Video case executed by IRS Criminal
22 Investigation and a number of other agencies
23 that led to arrests in I believe over
24 30 countries. There were a number of children
25 that were saved. It was the largest what's know

1 as CSAM material, child abuse material, that was
2 shut down in history which was coordinated with
3 many countries. There were specific parallel
4 actions by the department of justice in OFAC in
5 relation to North Korean hacking and hacking
6 that they had done in relation to cryptocurrency
7 exchanges. The volumes are getting close to, I
8 would say, about between 1.3 and \$1.5 billion in
9 2020. And one of the things that I'm regularly
10 asked is why are we seeing all of this now. It
11 is not because there is a more illicit activity
12 in the cryptocurrency space. We are in fact
13 seeing less illicit activity in the
14 cryptocurrency space as compliance has been
15 ushered in and regulation, et cetera. But the
16 capabilities of law enforcement and
17 investigators have improved substantially.
18 Based on my estimates, which are skewed in the
19 sense that I only know the information that I do
20 in relation to the number of users that we have,
21 I would say we have about 34 times as many
22 investigators in the US that are utilizing
23 Chainalysis than they are in Canada, for
24 example. So I think resources and accessibility
25 have been the primary driver coupled with

1 expertise that has certainly been developed and
2 the great investigators in law enforcement that
3 you have in the US that has driven a lot of
4 those successes, but I expect that that can be
5 duplicated in any place when those resources are
6 applied.

7 Q Would you say that the increased regulation and
8 in turn increased availability of KYC
9 information that allows law enforcement and
10 others to connect a wallet to a particular
11 individual, would you say that that has played a
12 role in this increase?

13 A I would say yes. I would say yes. I mean, in
14 an ideal world the way in which successful
15 investigation occurs is by following the money
16 and investigating wallets in the transaction
17 history. And I don't know if I referenced this
18 before, so please apologies if I have. But they
19 would follow it to an exchange and then by way
20 of [indiscernible] or MLAT, if they had to
21 execute that in relation to engagement with a
22 foreign country, if we're talking about the US,
23 for example, depending upon the relationship
24 that they have they would then be able to obtain
25 the associated KYC and PII of those bad actors.

1 That is how it should look like and how it
2 should work in practice successfully.

3 Q In Canada there's also been a number of
4 notorious samples of exchanges, including
5 probably the biggest story here is QuadrigaCX.
6 What can you tell us about that without getting
7 into any areas of current law enforcement action
8 and what insight does Chainalysis have on what
9 happened there?

10 A I know there are still a number of active
11 investigations in many different countries in
12 relation to Quadriga. So the amount of
13 information that I can provide you is fairly
14 limited, unfortunately. But what I can tell you
15 is that the operator of Quadriga, Gerald Cotten,
16 you know, essentially stole the users' funds.
17 Not essentially, he did. He stole the users'
18 funds. What we can tell you is in relation to
19 the associated activity based on some of the
20 illicit activity he was already involved in, he
21 could not gain access to banking. He became
22 engaged with some OTC brokers that were less
23 than savory and there has been a lot of
24 associated activity that has been followed all
25 over the world.

1 Q In using the Reactor software, particularly in
2 the context in which law a enforcement agent
3 might be using the Reactor software, does the
4 software have insight into transactions that are
5 operating only inside the exchange, so back and
6 forth between clients within the exchange?

7 A What we would call activity in transit. You'll
8 have to forgive me. I don't want to give an
9 inaccurate answer here. My instinct is to
10 supply and answer, but I would prefer to refer
11 bang to you once I'm able to get a confirmation
12 on how that works.

13 Q That's fine. We certainly wouldn't want you to
14 speculate on an answer that you don't have the
15 knowledge on at this moment.

16 MS. ROSE: So subject to any questions from you,
17 Mr. Commissioner, those are my questions for
18 Mr. Spiro.

19 THE COMMISSIONER: Thank you, Ms. Rose. No, I don't
20 have any questions.

21 MS. ROSE: Okay. My understanding is that the
22 Province of BC will be the next counsel asking
23 questions of Mr. Spiro and their allotment of
24 time is 20 minutes.

25 THE COMMISSIONER: Yes. Ms. Chewka.

1 MS. CHEWKA: Yes, thank you, Mr. Commissioner.

2 **EXAMINATION BY MS. CHEWKA:**

3 Q Morning Mr. Spiro. Can you hear me okay?

4 A I can.

5 Q Excellent. Thank you. I'm going to pick up
6 where my friend Ms. Rose left off and focus all
7 my questions on the regulatory framework and so
8 my first question is whether or not it's fair to
9 say that virtual assets is a complex area that's
10 moving or evolving fairly quickly.

11 A I think that that is an appropriate assessment.

12 Q In particular would you say that the risks
13 associated with virtual assets are also
14 constantly changing?

15 A To a degree. To a degree I think that's a fair
16 assessment. I think that the technology, as I
17 mentioned, is evolving quickly and we are seeing
18 new use cases and instances where there may be
19 additional risks. There are a lot of parallels,
20 though, in relation to illicit finance and
21 illicit activity that we see in this space that
22 you would see in traditional financial services
23 as well, so I think there are a number of
24 constants that will be maintained.

25 Q And in your experience have the law enforcement

1 agencies that you've dealt with kept pace with
2 those changes?

3 A In my experience what we've seen is that
4 globally law enforcement agencies by and large
5 were kind of behind the curve in relation to
6 this. I think it has been a catchup game. I
7 think some of them have been evolving quickly
8 and adapting and kind of building out their
9 capabilities and I think others are still
10 developing those capabilities.

11 Q For those that have been evolving quickly, I
12 understand that you had mentioned in your
13 evidence resourcing and training. Is that sort
14 of the key to success for law enforcement
15 evolution in this area?

16 A I think so. I mean, I can just speak again to
17 the capability of blockchain forensics and the
18 success stories that we've seen this year. You
19 know, part of that, I mean it's a combination of
20 things. There has been robust training, right,
21 of those agencies, you know, rapid expansion in
22 relation to those users and those that become
23 what we like to call power users. And so
24 they're coupling the expertise that they're
25 learning about the activity with the products

1 and with the training and then they're just
2 seeing, you know, almost unprecedented results,
3 I would say. So yes.

4 Q I understand from your evidence and as you just
5 explained it now that these law enforcement
6 agencies are using your software as an
7 investigative tool. Is that a fair assessment
8 of how they're using it primarily?

9 A Yes.

10 Q And so am I correct in saying that law
11 enforcement agencies are using your services
12 primarily after the alleged criminal activity
13 has occurred?

14 A For law enforcement explicitly I would think
15 that's probably accurate. However, they can
16 identify other potential leads and intelligence,
17 right, in relation to other activity which we do
18 see regularly as well. So they may be working
19 on specific activity, a specific case. They may
20 identify a number of associated wallets, for
21 example, and individuals, a larger network, more
22 activity which leads to more success.

23 Q So while it's primarily a reactive tool it can
24 have preventative uses as well?

25 A I think it certainly has preventative uses. I

1 mean, we've seen that many times as well.

2 Q Now, in your evidence you also talked about the
3 FINTRAC reporting requirements under the
4 PCMLTFA, and is it is fair to say that those
5 reporting requirements are occurring again after
6 suspicious transactions have occurred?

7 A No, some of those reporting requirements are not
8 connected at all to suspicious transactions.
9 They're connected to transaction thresholds, in
10 fact. Some of that aligns directly with the
11 travel rule, for example, that we have seen come
12 from the Financial Action Task Force and any of
13 that kind of information would support potential
14 investigations, right, because it provides
15 additional information and ease of accessibility
16 to law enforcement and investigators and
17 regulators, but it is not all connected to --
18 directly to, in relation to recordkeeping,
19 directly to suspicious activity.

20 Q Would you say that those reporting requirements
21 are again more reactive in nature if we're
22 trying to draw this distinction between
23 preventative and reactive, or would you say also
24 has a preventative result?

25 A I think it is a preventative intended result. I

1 think when it comes to recordkeeping and those
2 kinds of requirements, there does always need to
3 be a balance between what the impact is on
4 business function and, you know, harkening back
5 to something you hear regularly which is the
6 cost of compliance. So what the impact is on
7 those entities in the private sector to be
8 compliant with these things versus what
9 potential information it provides and the,
10 again, financial integrity it potentially
11 provides. So I do think that it needs to be
12 taken into account. You know, regulation is a
13 tricky thing because if it becomes too
14 draconian, which I'm not saying what this is at
15 all, but if it does become that way in relation
16 to competition, those that fall under that remit
17 will have potential problems, right, being
18 competitive in those in other jurisdictions
19 even.

20 Q In your evidence again today you have emphasized
21 the importance of realtime monitoring as part of
22 the strategy to addressing illicit activity. Is
23 that a fair assessment of your evidence today?

24 A Yes.

25 Q And based on your experience what additional

1 steps could be taken beyond the KYC requirements
2 that you had mentioned to prevent or mitigate
3 some the risks that are associated with virtual
4 assets?

5 A So obviously enhancing implementation of
6 regulation would be one thing; right?
7 Developing those compliance essentials, having
8 those programs in place. Having policies and
9 procedures, having red flags and typologies,
10 integrating that type of information into your
11 organization so you can identify that.
12 Identifying those kind of risks, doing your
13 internal risk assessment. The next step that
14 hasn't really been discussed which I think is an
15 important one, and we've only seen that this
16 really applied in very few jurisdictions thus
17 far, but it's an extremely important, is all
18 these regulatory requirements are now being
19 relayed and identified. So for exchanges that
20 have not been subject to regulation before or
21 have no requirements, they are putting the
22 program in place, right, so they will have the
23 compliance officer, the compliance program, you
24 know, all those things that I've mentioned a few
25 times today.

1 Implementation is one thing, but what's
2 known as enterprise risk management is seen as
3 the next iteration, right, which is where you
4 conduct these audits and these audits are
5 required to identify how successfully the
6 program functions. To identify gaps, to
7 identify potential vulnerabilities, different
8 kinds of testing conducted, seeing how effective
9 your program is. And that ongoing long term is
10 going to be extremely important and beneficial
11 because the carrot, for lack of a better term,
12 in many jurisdictions right now is if an
13 organization puts a program in place, they can
14 then get registered successfully and potentially
15 licensed to operate; right? But you want this
16 in perpetuity to be successful. You want to
17 make sure this is continued and that the upkeep
18 occurs, so I think that is the next step that's
19 important as well.

20 Q You had mentioned that with this enterprise risk
21 management that there are a couple of
22 jurisdictions. Are those the ones that are
23 implementing this next step, and if so, which
24 jurisdictions are doing that?

25 A So there are some that are more advanced, I

1 would say, just in relation to not only to
2 releasing the regulation but highlighting things
3 like enterprise risk management. The monetary
4 authority of Singapore comes to mind. In
5 relation to what I'd say are some of the most
6 advance regulatory regimes I think FinCEN for me
7 is probably the best example. FinCEN put out an
8 extremely prescriptive guidance around virtual
9 assets in 2019. They have put out multiple
10 advisories specifically in relation to virtual
11 assets. They have a program called FinCEN
12 Exchange wherein they bring the public sector
13 and the private sector directly together to
14 address specific issues and they've done that
15 for virtual assets. They recently did this for
16 ransomware as well, business email compromise I
17 believe also. These programs are extremely
18 important for information sharing in a closed
19 session and developing new tools. And then they
20 have as a regulator a specific unit that focuses
21 on virtual asset enforcement, and that to my
22 knowledge is fairly unprecedented also, wherein
23 within the FIU they have that specific group
24 that specifically focuses on that kind of
25 activity.

1 Q Now, you mentioned FinCEN. Are there other
2 jurisdictions that we should be looking to for
3 cross-jurisdictional learning purposes in your
4 experience?

5 A I think there's a number. I think the monetary
6 authority of Singapore is a good one. I think
7 Japan is a good one. I think the UKFCA has
8 built out a good regime in relation to their
9 requirements. I mentioned the US. I think the
10 program itself that's been developed by ADGM,
11 Abu Dhabi Global Markets, is robust as well.
12 Those would be off the top of my head.

13 Q Is it there anything that these jurisdictions
14 are doing in particular that you would say
15 beyond what you've already given evidence on
16 that are like the hallmarks of a robust
17 regulatory regime in this area?

18 A I think that they have been -- they took a
19 proactive approach initially, so I think the
20 regimes that they've built out are just, you
21 know, extremely strategic. They've put a lot of
22 time and effort into not only identifying the
23 risks but the particulars that will be important
24 to successful functionality in the country;
25 right? While still in many cases trying to

1 support invasion. So you know, I will add some
2 of them are not functional technically yet.
3 They have just built out these regimes that I
4 think are very good as a benchmark.

5 Q I'll ask a specific question based on the
6 testimony of Sergeant Vickery yesterday.
7 Yesterday she testified that in her view one
8 solution or maybe a part of a solution would be
9 to have financial institutions deal directly in
10 virtual assets or with virtual assets and
11 eliminate third party public exchanges. So I'm
12 going to ask a two-part question here. The
13 first part is in your view whether or not
14 Sergeant Vickery's proposed solution is viable
15 or in your opinion whether there is still a role
16 here for a unique independent regulator of third
17 party public exchanges?

18 A Well, right now there is not a unique
19 independent regulator for these kinds of
20 businesses; right? Usually they roll into the
21 same regulatory regime that you have for other
22 kinds of financial services. I think generally
23 that makes sense. I do think that is a
24 potential option. That you could have, right,
25 if you had the resources in a country to have

1 specific regulation that is applied just
2 specifically to this space, you could do that.
3 I think our end goal and our motto is building
4 trust in blockchains. When I say that what I
5 mean is we are a unique intermediary if you
6 think about us between the public and the
7 private sector and you have data that is used
8 collectively to build trust in this ecosystem.
9 For larger adoption to occur outside of what
10 we've seen thus far, right, even though there
11 are promising developments eventually what you
12 would like is institutional adoption, in the
13 sense that there would be the accessibility
14 between fiat, between using banking, between
15 using cryptocurrency, and that fusion would
16 eventually occur I think for this really to take
17 off and develop in the way that it has the
18 potential to do so. I don't think necessarily
19 one entity needs to swallow another. I don't
20 think traditional banking needs to swallow up
21 the cryptocurrency space or the organizations.
22 They have subject matter expertise and they have
23 brought very unique thinking and technical
24 advancements that I don't think could be
25 replicated or duplicated easily by a big bank.

1 So I think cohesively working together is
2 probably ideally what happens. But for the
3 financial institutions, for the large financial
4 institutions, you are seeing them to start to
5 dip their toes in. But for them to become more
6 comfortable, really more comfortable with the
7 space, it comes from successful regulation and
8 identifying the fact that it is a safe ecosystem
9 I think we are seeing progress there, but I
10 think it has to get there for you to see more of
11 that kind of development.

12 I will add one other thing, or please
13 proceed, actually. This is not -- what I would
14 add in relation to investigations, however, is
15 conceptually the idea of a national centre
16 that -- and I mean this for many different
17 jurisdictions where they potentially have the
18 resources to do it this is I think potentially
19 valuable, because again with the cryptocurrency
20 ecosystem existing in the way in which it does
21 and again the speed, the velocity and the nature
22 of it, I think having centralized resources, law
23 enforcement capabilities to work and tackle on
24 this project is potentially attractive. I'm not
25 saying necessary but I think potentially

1 attractive.

2 Q Are there are any potential disadvantages to
3 regulating this area? And so I'm thinking, for
4 example, of the stifling of invasion. You've
5 also mentioned things like you can become too
6 draconian. Can you elaborate on the potential
7 disadvantages or at what point we go too far
8 potentially in your view.

9 A Yeah, I think that invasion has driven so many
10 amazing things right in relation to digital
11 payments and Fintech, what's known as Fintech
12 recently, right, and will continue to do that
13 and in fact it's moving more quickly than I
14 would have expected, which is amazing. But two
15 things are happening. One, those innovators and
16 those that are developing this technology
17 sometimes are not soliciting the feedback and
18 having the kind of engagement that they should
19 with the regulators and then they're running
20 into major regulatory hurdles, right, because,
21 again, if something becomes dangerous even if
22 it's brilliant and unique there have to be some
23 controls. There has to be protection, consumer
24 protection, safety, these kinds of thing. So
25 that is on the one hand. But on the other hand

1 if you bring in regulation too stringently, the
2 innovators, the biggest innovators when they
3 realize that they cannot develop those
4 technologies and exist in the jurisdiction they
5 are in, they will leave. They will go to places
6 where they can, where they can develop and they
7 can deploy the technology effectively. That is
8 something that will happen. It certainly is a
9 concern, it's a concern that I've heard from
10 domestic operators in the US before and I've
11 heard it from other jurisdictions as well, so
12 it's something to take into account. It
13 requires a balance.

14 Q And my last question for you today is that I
15 understand from your evidence that bad actors in
16 this area can be quite savvy or adaptable. And
17 in your view will regulation prevent potential
18 illicit activity or will it simply shift that
19 activity elsewhere and how do we stay ahead of
20 that curve?

21 A So think of it as bad actors are always looking
22 at a fence, probing the fence for
23 vulnerabilities or holes to exploit. You have
24 that in the traditional financial services
25 ecosystem. You have that in this ecosystem as

1 well. So that will exist. I think there would
2 not be the capability -- people have mentioned
3 before well, if you do this or you do that
4 you'll just push this complete black market or
5 grey market into existence. And there is
6 potential for something like that to develop, to
7 be fair. You could have that. But what I hark
8 back to the fact that without the accessibility
9 and the liquidity that is connected to this
10 global ecosystem to those that have access to
11 banking and otherwise, there's not going to be
12 the kind of value associated with doing it or
13 access wherein it would be feasible long term
14 and sustainable, I think is the better word that
15 I'm looking for. It could happen. There are
16 certain particulars wherein you could see a push
17 to those kinds of markets. I don't know how
18 large they could potentially grow. It is
19 something that could happen, but that's my
20 personal opinion.

21 MS. CHEWKA: Thank you. Thank you, Mr. Commissioner,
22 I have no further questions.

23 THE COMMISSIONER: Thank you, Ms. Chewka. I'm sorry.
24 Go ahead, Ms. Rose.

25 MS. ROSE: Mr. Commissioner, I believe our next

1 cross-examination will be conducted by
2 Ms. Jessica Magonet of the BCCLA and Ms. Magonet
3 has 25 minutes.

4 THE COMMISSIONER: Yes. Thank you, Ms. Magonet.

5 MS. MAGONET: Good morning, Mr. Commissioner. Thank
6 you. Everyone.

7 **EXAMINATION BY MS. MAGONET:**

8 Q Mr. Spiro, I have a few questions for you today.
9 Can you hear me?

10 A I can.

11 Q Excellent. My first questions concerns the
12 cryptocrime report produced by Chainalysis.

13 MS. MAGONET: If Madam Registrar could please pull
14 that up. That would be great. Actually not
15 this document but the cryptocrime report.
16 Though I will want to go to that document after.
17 Thank you. If you could please go to page 5.

18 Q So at the top of page 5 it says:

19 If the last few years have proven
20 anything, it's that cryptocurrency isn't
21 just for criminals. Polling shows that
22 adoption is increasing, as 18 percent of
23 all Americans and 35 percent of American
24 millennials have purchased cryptocurrency
25 in the last year. Mainstream financial

1 institutions like JP Morgan Chase are
2 getting involved. Popular retailers like
3 Amazon and Starbucks now allow customers
4 to pay in Bitcoin."

5 You would agree with this statement?

6 A I am just going to read it again.

7 Q Oh, no problem.

8 A Yes, I think we're seeing more adoption. In
9 fact if you would reference the price of bitcoin
10 today and all of the press we're seeing I think
11 it tracks with that statement, yes.

12 Q Thank you.

13 MS. MAGONET: And, Madam Registrar, if you could
14 scroll down a bit yes.

15 Q So further down on the page just below the graph
16 it says:

17 "Illicit transactions still make up a
18 small share of all cryptocurrency activity
19 as just 1.1 percent."

20 And you would agree with this statement?

21 A This was as of 2019?

22 Q Yes.

23 A I think potentially slightly lower even this
24 year, although you can't quote me on that, but,
25 yes, I agree with this, yes.

1 Q And earlier today in your testimony I just
2 wanted to confirm you said the amount of illicit
3 activity in the cryptocurrency space is actually
4 going down; is that correct?

5 A Yes.

6 Q Thank you.

7 MS. MAGONET: Madam Registrar, if you could go to
8 page 6 of this report.

9 Q And I just want to find the sentence I'm looking
10 for. So just below the graph here it says:

11 "Were it not for just three separate
12 large-scale Ponzi schemes, the crime would
13 account for just .46 percent of all
14 cryptocurrency activity."

15 Understanding this is based on a 2019 report you
16 would agree with this statement?

17 A Yes. From 2019, yes.

18 Q Great. And you would agree that this report
19 demonstrates that the majority of cryptocurrency
20 gained through criminal activity just goes to a
21 small segment of criminals?

22 A Yes. That's accurate, I would say.

23 Q Great. Thank you. Those are my questions with
24 respect to this report. I now have some
25 questions related to Chainalysis's work with law

1 enforcement. As a first question can you tell
2 me which police agencies that Chainalysis has
3 contracts with in Canada?

4 A I'm not sure based on confidentiality that we
5 have if I can do that. Not only is that what I
6 would say, but full disclosure that kind of
7 falls outside of my remit in relation to the
8 work that I do directly. So apologies.

9 Q No, that's fine. I certainly wouldn't want to
10 ask you to give evidence outside of the scope of
11 your knowledge. Are you able to tell me whether
12 Chainalysis has contracts with any law
13 enforcement agencies in Canada and in particular
14 in British Columbia?

15 A I believe I can say that we do have contracts
16 with law enforcement in Canada, yes. I can't
17 tell you where explicitly, but I believe we do
18 have them in Canada, yes.

19 Q And do you know if Chainalysis has contracts
20 with other government agencies or national
21 security agencies in Canada?

22 A Again, to my knowledge I don't know the scope in
23 relation to the number of agencies. I know that
24 we work with law enforcement in Canada. It is
25 certainly possible that we work with additional

1 government agencies in Canada. Probably likely
2 I would say as well, in fact.

3 Q Thank you. Is the Chainalysis Reactor software
4 a software that can be purchased by companies as
5 well as law enforcement?

6 A Yes.

7 Q Can it be purchased by individuals?

8 A No.

9 Q Okay. And what limits if any does Chainalysis
10 place on a customer, whether it be law
11 enforcement or a company, who purchases the
12 Chainalysis Reactor software in terms of what
13 they can do with the data available through that
14 software? Are there any limits placed on that?

15 A I don't know if I understand the question. Are
16 you saying do we put controls around what our
17 users can do with the data?

18 Q Exactly. That's my question.

19 A I would assume it varies depending upon the kind
20 of entity that we work with. In some cases I
21 would assume correctly that there will be
22 controls in relation to what can be done with
23 the data.

24 Q Do you think in some cases there would be no
25 controls?

1 A I cannot speak one way or the other to if there
2 were or were not controls in relation to our
3 customers. Again, unfortunately, you know, I
4 handle regulatory affairs and policy for our
5 organization. I am familiar with our products
6 and services. I'm familiar loosely in relation
7 to scope with the kinds of entities that we work
8 with, but in relation to the specific mechanics,
9 functionality, those kinds of things in relation
10 to contracting, which is a lot of what I think
11 you're discussing and mentioning, I do not have
12 visibility into that kind of information.

13 Q No problem. Thank you. So when Chainalysis
14 works with law enforcement is the way it usually
15 works that law enforcement is purchasing the
16 Chainalysis Reactor software?

17 A With law enforcement in many cases they would
18 purchase our software, yes.

19 Q And they might also obtain contracts-based
20 investigative services from Chainalysis as well.
21 Could that happen?

22 A It could.

23 Q Thank you. Madam Registrar, if you could please
24 pull up the PDF document of the Chainalysis
25 website for the Chainalysis Reactor page.

1 Mr. Spiro, do you recognize this. This is a
2 print to PDF of the Chainalysis Reactor tab on
3 the Chainalysis Reactor website.

4 A It does look like Reactor, yes.

5 Q Okay. Excellent.

6 MS. MAGONET: Madam Registrar, if you could please
7 scroll down a bit to the bottom of that page.

8 Q Here it says that Chainalysis Reactor allows you
9 to:

10 "Enter any cryptocurrency address to learn
11 which entity controls the wallet and
12 discover related addresses."

13 Would you agree that this is what Chainalysis
14 Reactor allows you to do?

15 A It allows to you identify entities, yes. Not
16 individuals but you can identify entities, yes.

17 Q And what is meant by entities? Is that a
18 company? Is that a group of people?

19 A It would not be a group of people. It would be
20 you can identify what we would consider to be
21 entities on the blockchain. It could be a
22 company. It could be a kind of service. It
23 could be a darknet market. It could be
24 something that is unknown, right, where we have
25 not been able to make an attribution or define;

1 we just know there is a number of connectivity
2 there, there's a number of different kinds of
3 services in this space. It could be other kinds
4 of services that exist in this space like
5 gambling site, et cetera. So there's a number
6 of different kind of entities that could be
7 identified.

8 Q So the Reactor allows you to say which entity is
9 controlling a cryptocurrency wallet; that's
10 correct? Sorry it go over this again. I just
11 want to make sure I understand.

12 A Yes.

13 Q Okay. Great. Does the Chainalysis Reactor
14 software allow users to determine the location
15 of this entity?

16 A If we have information on the entity in relation
17 to where it's domiciled, I wouldn't hark to
18 Reactor; I would hark to Kryptos wherein we have
19 some of that registration and other kinds of
20 information. But I --

21 Q Could -- sorry, please go ahead.

22 A I would warn, because it sounds like we're
23 getting into territory where you are starting to
24 ask questions about functionality of our
25 products. And so what I would say is one,

1 harking to the effect there are confidentiality
2 agreements and proprietary information that I
3 potentially couldn't share, but more to the
4 point further and what I would call most
5 concerning for why I don't think I could
6 answer certain types of questions if we're going
7 in that direction is because this is public
8 testimony and because this is public testimony
9 there is a potential that anyone could watch
10 this, including bad actors and money launderers
11 and potentially identify information that would
12 contribute to their efforts. In fact I can cite
13 specific cases where this has happened recently
14 and then published. So I think that would be
15 the antithesis of what we're doing this hearing
16 for and why I have chosen to participate and
17 provide testimony today. So if we are going in
18 that direction I would have to say that I
19 respectfully not be able to speak about those
20 kinds of capabilities, if we did or didn't have
21 them.

22 Q I certainly understand that and I wouldn't want
23 to you to have to answer any questions that you
24 don't feel positioned to answer. But just so
25 you understand the thrust of my questions I'm

1 just trying to get a sense of not the specifics
2 of the types of information that are available
3 through the Chainalysis Reactor but at a more
4 higher level scale. So maybe what I could do,
5 then, is to return to something I believe you
6 said earlier to Ms. Rose or perhaps it was
7 Mr. Place who said this but that Chainalysis is
8 providing analysis of the blockchain which is
9 publicly available data; is that correct?

10 A Yes.

11 Q But Chainalysis isn't just providing -- or the
12 Reactor isn't just providing analysis of the
13 blockchain, it's also integrating other data
14 sources. Is that accurate?

15 A Yes. We use human intelligence, heuristics a
16 number of different kinds of information to
17 provide the data that we provide. That is
18 correct.

19 Q And on this document here it says it alludes to
20 the fact that the Chainalysis Reactor uses open
21 source intelligence data. That's correct?

22 A There is some open source intelligence data that
23 is included. It is not referenced in relation
24 to all of the wallets, all of the attributions;
25 there is just some that is contributed and

1 contained in relation to specific transactions.

2 Q And just to speak at a high level, not the
3 specific data that Chainalysis is using but for
4 the benefit of any people here who may not know
5 what open source intelligence data is, that
6 could include things like your social media
7 page, your media report, commercial data from a
8 private database, data purchased from data
9 brokers. Is that accurate?

10 A No, any of the information that would be
11 included and again I'm going to curb this after
12 I provide the following because, again, I don't
13 want to provide any proprietary information in
14 relation to what we use or who we work with.
15 Any of the information that we are using to my
16 knowledge is actual open source information.
17 And when you talk about proprietary database and
18 other kinds of information, I don't believe that
19 would be considered to be open source. I could
20 be wrong. We do solicit information from a
21 number of different resources that we use. We
22 also have a number of partners that we work with
23 to solicit the different kinds of information.

24 Q Okay. Thank you. Would you agree that open
25 source intelligence data, while open source so

1 publicly available, may still be considered
2 private by an individual. So for example, a
3 post to a social media page, even if that could
4 fall within the scope of OSINT, a person
5 publishing it might consider it to be private?

6 A Yeah, I mean data privacy and data protection
7 are something that we are intimately familiar
8 with. You know, it is something that I
9 understand. I will add that there is a historic
10 conflict that it seems you're starting to work
11 around which is there is a conflict with data
12 privacy and data protection and potentially with
13 the anti-money laundering and CFT laws. This is
14 historic. You see it in Europe with GDPR in the
15 AML laws there. You see in it other places
16 potentially as well. It certainly is
17 potentially something that exists. That is not
18 something -- that is not something that I think
19 is potentially relevant in relation to the kind
20 of work that we do, but again, because I can't
21 focus in on any of the specific kinds of
22 information that we solicit I unfortunately
23 don't think I can provide you any additional
24 information on that.

25 Q Thank you. Are you able, and it's okay if

1 you're not, but are you able to tell me if
2 Chainalysis ever purchases data from data
3 brokers?

4 A Off the top of my head I am not sure. I do not
5 know. I believe it is possible, but off the top
6 of my head I'm not sure. But entirely possible,
7 probable.

8 Q Thank you. And is the Chainalysis Reactor able
9 to link a cryptocurrency wallet to a specific IP
10 address? Is that something you're able to tell
11 me?

12 A That again, what you're talking about are
13 specific functions and features and I cannot
14 talk to you about any of those things today,
15 unfortunately, so my apologies.

16 Q Thank you. Does Chainalysis ever disclose
17 personal information by selling its products to
18 the entities that purchase it?

19 A Sorry, could you ask the question again.

20 Q Certainly. So does Chainalysis through the sale
21 of its products ever disclose personal
22 information to the entities who are purchasing
23 them or information you might consider to be
24 sensitive?

25 A Do we disclose PII or sensitive information to

1 our clients?

2 Q Sorry, perhaps I'll rephrase my question. When
3 a client purchases Chainalysis software such as
4 the Chainalysis Reactor is Chainalysis
5 effectively giving them access to personal
6 information?

7 A No. This is pseudo-anonymous addresses that are
8 all public on the blockchain.

9 Q Okay. Sorry, I didn't mean to cut you off.

10 A Yeah, all of this information in relation to the
11 blockchain in these wallets, A, they are
12 pseudo-anonymous so you cannot identify who the
13 owner is. We don't ever touch any of that kind
14 of information.

15 Q Thank you. Does Chainalysis have any
16 requirement that it applies before it will allow
17 law enforcement -- sorry, let me think about how
18 to reformulate this question. Does Chainalysis
19 ever require law enforcement to seek a
20 production order prior to providing data to law
21 enforcement?

22 A I mean law enforcement would have to be a client
23 of ours to be using our services. There are
24 instances where trials are provided to any kind
25 of client that we have, right, before purchasing

1 a service potentially.

2 Q But do you ever require law enforcement to seek
3 a production order or a warrant before
4 disclosing information to them?

5 A If -- are we talking about if they are our
6 client or if they are not a client of ours?

7 Q If they are your client.

8 A What kind of data would they -- you're saying --
9 I don't know if I understand the question. I
10 have to apologize. In relation to the usage of
11 our services?

12 Q Certainly. My apologies if it wasn't clear. So
13 perhaps this context, usually when law
14 enforcement is seeking a person's personal
15 financial data from a bank, for example, they
16 can't just walk in and get that. Like, they
17 would need a production order first given the
18 sensitivity and privacy of the type of
19 information. And I was wondering if there is a
20 similar process when working with Chainalysis or
21 if you take the position that this is all
22 publicly available data so that's not necessary?

23 A Yes. It's not necessary in relation to their
24 use of our data. I think if they were to
25 solicit data from exchanges, that would exist.

1 Q Okay. Thank you. And earlier you alluded to
2 the fact that cryptocurrency is highly
3 traceable. Would you agree with that statement?

4 A I would say that it provides a transparency, a
5 traceability, providence. That certainly
6 exists, yes.

7 Q Would you agree that cryptocurrency when
8 combined with blockchain analysis technology
9 presents an unprecedented opportunity for
10 financial surveillance?

11 A I would not call it financial surveillance. I
12 would talk about financial integrity, which is
13 important for any kind of functional ecosystem.
14 We exist as a white hat organization. As I
15 mentioned before we stop proliferation
16 financing, human exploitation, child
17 trafficking, terrorism financing this year. You
18 name it, we have been able to assist in relation
19 to that. And so unless somebody in turn doesn't
20 want that to exist and wants to allow all of
21 that activity unimpeded, this is essential and
22 extremely valuable. That would be my opinion.

23 Q Thank you. You would agree that Chainalysis
24 Reactor can be used in not only a reactive
25 manner but also in a proactive manner to

1 predict -- well, perhaps not predict but detect
2 activity that perhaps law enforcement didn't
3 have a pre-existing interest in or awareness of?
4 A I think it's law enforcement's duty to have an
5 interest in illicit activity, but they would
6 only be following the flow of funds in relation
7 to illicit activity. They wouldn't be looking
8 for -- you know, in relation to the scenarios
9 that I'm familiar with, they would not be just
10 trolling along on the blockchain wasting
11 valuable hours and resources.

12 Q Thank you. And earlier when Ms. Rose was asking
13 you about changes you think would be beneficial
14 to Canada's anti-money laundering and terrorist
15 financing laws with respect to virtual assets, I
16 just wanted to make sure I understood something
17 that you said. I believe that you said that
18 increased reporting would be beneficial given
19 its preventative, potential preventative uses.
20 Is that correct?

21 A Increased reporting as in a record? I mean,
22 there are recordkeeping requirements that are in
23 existence that require increased recordkeeping.
24 Increased reporting is something else, though.
25 That's something completely different. You

1 potentially run into an issue when there's too
2 much reporting in relation to STR where they
3 can't effectively be worked through. They
4 should be targeted. It should be targeted
5 information that supports law enforcement and
6 regulators in relation to their efforts. So
7 volume, yeah, volume is not necessarily a good
8 thing at all. If you're starting from nothing
9 it's important to continue to begin to build
10 that, but you know, I would say it needs to be
11 targeted.

12 Q Thank you. I just have two or three last
13 questions for you because I know I'm running out
14 of time. Are you able to tell me how much
15 Chainalysis's contracts with policing and
16 intelligence agencies in Canada are worth, or is
17 that outside the scope of your knowledge?

18 A It's outside the scope of my knowledge. My
19 apologies.

20 Q No worries. And do you know in Chainalysis
21 employees have ever acted as experts in criminal
22 prosecutions in Canada?

23 A I do not. I should say I do not know.

24 Q And do you know if there are any other ways that
25 Chainalysis would receive revenue from law

1 enforcement or government within Canada?

2 A It would only be from contracts.

3 MS. MAGONET: Okay. Thank you. Those are my
4 questions. Thank you very much.

5 THE COMMISSIONER: Thank you.

6 MS. ROSE: Mr. Commissioner, I'm hoping that we might
7 take a further short break of perhaps
8 ten minutes now to address an issue that has
9 arisen if you're amenable to that.

10 THE COMMISSIONER: Yes, all right. That's fine,
11 Ms. Rose. Ten minutes.

12 MS. ROSE: Sorry, Mr. Commissioner. I just wonder it
13 if you wish to give the witness the usual
14 caution about not discussing his evidence during
15 the break.

16 THE COMMISSIONER: Yes. All right. Thank you.
17 Mr. Spiro, it's a common rule I'm sure in the US
18 as well as in Canada, but when you're under
19 cross-examination you're not permitted to speak
20 with anyone about your evidence. So I just
21 indicate that rule is in place for you. Thank
22 you.

23 THE WITNESS: Thank you.

24 THE COMMISSIONER: All right. We'll take
25 ten minutes.

1 THE REGISTRAR: This hearing is stood down for
2 ten minutes until 12:56 p.m. Please mute your
3 mic and turn off your video. Thank you.

4 **(WITNESS STOOD DOWN)**

5 **(PROCEEDINGS ADJOURNED AT 12:46 P.M.)**

6 **(PROCEEDINGS RECONVENED AT 12:56 P.M.)**

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

9 **JESSE SPIRO, for the**
10 **commission, recalled.**

11 THE COMMISSIONER: Thank you, Madam Registrar. Yes,
12 Ms. Rose.

13 MS. ROSE: Mr. Commissioner, before we move on to the
14 next participant's examination I wanted to
15 indicate on the record something here. As you
16 know, both Mr. Spiro and Mr. Place are here from
17 Chainalysis and the focus of the evidence today
18 has been on Mr. Spiro, although we did have
19 Mr. Place attending in particular to facilitate
20 the demonstration of the Chainalysis products.
21 Unfortunately, Mr. Place has been feeling
22 unwell. He currently has a fever and he is
23 unable to continue today, and so we are hopeful
24 that we can cover the ground as necessary with
25 Mr. Spiro, but in the event that Mr. Gratl for

1 Transparency International considers that there
2 are outstanding issues at the end of this
3 cross-examination with Mr. Spiro, I suggest that
4 we address it at that time because I do know
5 that my colleagues had contacted Mr. Place to
6 inquire about him attending, but I'm
7 understanding that that's not possible at this
8 time.

9 THE COMMISSIONER: Okay. All right. Thank you,
10 Ms. Rose. Mr. Gratl, are you ready and able to
11 proceed with Mr. Spiro?

12 MR. GRATL: I am, thank you, Mr. Commissioner.

13 THE COMMISSIONER: Thank you.

14 **EXAMINATION BY MR. GRATL:**

15 Q So, Mr. Spiro, Chainalysis clients include
16 virtual assets service providers including
17 crypto-exchanges; is that right?

18 A That is correct.

19 Q And then other clients include financial
20 services businesses, including banks and hedge
21 funds and private equity groups; is that right?

22 A I believe so, yes.

23 Q Okay. And in terms of those financial services
24 businesses it's not possible to tell on the face
25 of it whether those entities are acting as

1 over-the-counter brokers; is that right?

2 A Well, to my knowledge I don't know of any bank
3 that is or financial provider that would be
4 acting as an OTC broker. There would be flags,
5 if you will, or tells in relation as I mentioned
6 before to large volumes associated with OTCs
7 wherever you are. So that activity would be
8 identifiable.

9 Q Yes, and you'll agree with me that 90 percent of
10 all volume in terms of cryptocurrency
11 transaction is now in excess of \$10,000; is that
12 correct?

13 A It could be potentially be accurate. Off the
14 top of my head I cannot confirm, but I know that
15 in relation to transaction volume it certainly
16 is plausible.

17 Q It's around 90 percent then, is it? Over, in
18 excess of \$10,000?

19 A That seems realistic. I would have to cite
20 specifics to be able to confirm definitively,
21 but that seems realistic.

22 Q And transactions in excess of \$1 million
23 constitute more than half of the entire dollar
24 amount of cryptocurrency transactions now;
25 correct?

1 A I don't know if I understand the question.

2 Q All right. Let's say you've got a total dollar
3 amount X of all cryptocurrency transactions in a
4 given month. Greater than half of that total
5 dollar amount consists of transactions in excess
6 of \$1 million; correct?

7 A I think you have to make the distinction between
8 what happens on chain as it pertains to services
9 and activity between services in those kinds of
10 entities and then there is unhosted activity as
11 well which is activity between wallets which
12 also exists. So you know, there's a lot of
13 different potential data components involved
14 there.

15 Q I'll just read from your report to 2010
16 geography of cryptocurrency.

17 THE COMMISSIONER: Can we put that up on screen,
18 Mr. Gratl.

19 MR. GRATL: Sure. At page 103, Madam Registrar,
20 please.

21 Q You'll see at the bottom, Madam Registrar, if
22 you could scroll down. "As of June" I'm
23 reading. June of 2020 I take it, Mr. Spiro.

24 "-- over 90 percent of cryptocurrency
25 transfer volume came from

1 professional-sized transfers above \$10,000
2 worth of cryptocurrency."

3 That's pretty --

4 A Yeah. Yes. So the distinction that I was
5 making is this is transfer volume that we're
6 talking about between entities; right? That's
7 all that I was saying. But obviously this is
8 our data, so confirmed.

9 Q Confirm. And then the following paragraph takes
10 this high volume of high worth transfers as an
11 indication that the ... That the area is
12 becoming more legitimate; is that right?

13 A Yes.

14 Q And then over on the following page you'll see
15 in the first full paragraph under the graph at
16 the last sentence:

17 "The increasing dominance of North
18 America's professional market since
19 December 2019 appears to be almost
20 entirely driven by transfers of \$1 million
21 or more worth of cryptocurrency, many of
22 which we believe are coming from
23 institutional investors."

24 Is that right?

25 A Yes.

- 1 Q And those institutional investors, I'm
2 suggesting to you some of them are your clients.
3 Am I wrong about that?
- 4 A No. You're not wrong.
- 5 Q And you keep track of which of your investors
6 are involved in these transactions in excess of
7 \$1 million?
- 8 A Yes, we would be able to follow the flow of
9 funds, yeah.
- 10 Q All right. And for those you don't keep records
11 of whether they're acting as OTC brokers, do
12 you?
- 13 A I don't think we keep explicit records in
14 relation to functionally how they are
15 interacting, no.
- 16 Q Sure. But all of those entities, banks, hedge
17 funds, private equity groups that are your
18 clients might be acting as OTC brokers but you
19 don't know whether that is so?
- 20 A That's not -- yeah, that's not a service that we
21 would provide. We will have a record of
22 transactions that have occurred, so we would
23 have a record in relation to high volume
24 transactions, to your point.
- 25 Q You might have a record of transactions, but a

1 lot of the records there wouldn't be records of
2 many different types of OTC transactions like
3 derivatives or transfers of paper wallets or
4 trust relationships, would there?

5 A There are some indicators in relation to
6 derivative transfers, but by and large I would
7 say no. That is not the kind of information
8 that we would -- that we produce.

9 Q Sure. Because they don't -- those types of
10 transactions, transactions that are derivative
11 of cybercurrency, that transactions where the
12 so-called paper wallet, which is just the key
13 and the password and trust relationships, those
14 don't make it into the blockchain; right?

15 A Yes, if it occurs offchain we are not going to
16 have a record of it. That is correct.

17 Q And those types of relationships, derivative and
18 trust relationships, are the types of
19 transactions in which sophisticated banks, hedge
20 funds and private equity groups specialize in
21 that type of transaction, don't they?

22 A Potentially. It falls outside of my area of
23 expertise in relation to those kinds of
24 financial services, but I assume they do a lot
25 of their business in those spaces.

1 Q All right. And then some of your clients are
2 governments; correct?

3 A That is correct.

4 Q Including some regulatory agencies?

5 A That is correct.

6 Q And then others are properly policing, either
7 domestic or international policing; correct?

8 A Correct.

9 Q And then other clients are defence contractors;
10 is that right?

11 A I ...

12 Q Military?

13 A We work with a wide swathe of different kinds
14 ever clients. The way that we usually define
15 publicly our clientele is between the public
16 sector, the cryptocurrency space and traditional
17 financial services, so we work with many
18 different kinds of entities in the public
19 sector.

20 Q Well, you work with the US Department of
21 Defence; right?

22 A If that information is public record. I would
23 have to check.

24 Q You're not sure whether you work with the US
25 Department of Defence?

1 A As I mentioned before in my previous testimony
2 in relation to the clients that we work with I
3 know that we have confidentiality agreements.
4 What I don't want to do is violate that kind of
5 confidentiality agreement which is why I'm
6 conscious of confirming any kind of information
7 or not confirming any information that might
8 exist.

9 Q Well, you should tell the people who are running
10 your website because you're currently
11 advertising for somebody to do sales to the US
12 Department of Defence.

13 A Well, if somebody is potentially going to do
14 sales with the US Department of Defence it
15 doesn't mean that they're currently doing them,
16 does it?

17 Q Is that your evidence? You're under oath, sir.

18 A Is what my evidence? I just provided my
19 evidence which is that we work with a myriad of
20 different kinds of government agencies.

21 Q You're not at liberty to reveal whether you're
22 working for the US Department of Defence? So --

23 MS. ROSE: Mr. Commissioner, Mr. Spiro has already
24 answered this question to the best of his
25 ability. He has advised that providing further

1 detail on this could reveal sensitive and
2 potentially propriety information and that there
3 could be implications for foreign law
4 enforcement regarding notification of these
5 details, and quite frankly this goes beyond what
6 is relevant to our mandate here with the
7 commission. We have not brought this witness
8 with the view to getting into this type of
9 commercial information from Chainalysis. We are
10 dealing with a witness who has not been brought
11 under subpoena as Mr. Spiro is resident in the
12 United States, and I would submit that the
13 witness has answered this question sufficiently
14 already.

15 THE COMMISSIONER: Well, he has in fact answered it.
16 He said that he isn't aware whether or not that
17 is public knowledge or whether or not it's
18 governed by confidentiality concerns, so I think
19 if you could move on, Mr. Gratl.

20 MR. GRATL: Thank you, Mr. Commissioner.

21 Q Chainalysis provides access to its data on the
22 basis of software as a service; is that right?

23 A We provide software as a service. Yes, we
24 provide software as a service. We also provide
25 other kinds of services as I mentioned as well.

1 Q All right. And I take it that what that means
2 is that your clients can't actually purchase the
3 Reactor software, they actually just access the
4 software by means of an internet connection; is
5 that right?

6 A Our clients can access our products in a number
7 of different ways and they can purchase them by
8 way of the internet. Utilization of the
9 internet, yes. Again I'm not in -- two things
10 that I should add. One, I'm not on the side of
11 the house, so unfortunately I'm not best suited
12 to answer those kinds of questions. But also in
13 relation to questions that pertain to things
14 like technical implementation and access, again
15 because of the proprietary nature of some of
16 that kind of information I cannot share it.

17 Q All right. I take it some of your clients,
18 though, access over the internet software that's
19 hosted on your servers?

20 A I believe that to be accurate, yes.

21 Q All right. And then in order to use the
22 software they have to sign a customer agreement;
23 is that right?

24 A Yes. I believe that's probably accurate.

25 Q And then the software -- by the -- by your

1 client?

2 A Sorry, you cut out there for a moment there.

3 Q Your software tracks the uses of the software by
4 the client. It logs, for example, the types of
5 searches that are conducted and so forth?

6 A I'm not privy to what kind of information is or
7 not captured in relation to our client's usage.

8 Q All right. For some customers, in particular
9 virtual asset service providers, they are
10 required to provide you with information about
11 their own clients in order to access your
12 database; correct?

13 A Potentially that could happen. Also if our
14 clients are -- if the client is using something
15 like the KYT software, they are integrating and
16 running transactions through that, right, so
17 information would be provided as a result of
18 that as well.

19 Q Sure. And so that would provide Chainalysis
20 with information that is held by, for example,
21 cryptocurrency exchanges, including the identity
22 of the owners of the wallets?

23 A No. We would never have any information
24 pertaining to the identities or any PII for the
25 owners of wallets or access to any of that kind

1 of information, nor do we want access to any of
2 that kind of information.

3 Q In addition to providing software as a service
4 Chainalysis also has an investigative team that
5 will actually participate in investigations with
6 law enforcement groups; is that right?

7 A That is correct.

8 Q And certainly while participating in those
9 investigations, it learns about the nature of
10 those investigations and the reasons sometimes
11 why suspects are being targeted?

12 A Our team supports both the public and private
13 sector in relation to investigations. By and
14 large the information that is provided is in
15 relation to specific wallets. If additional
16 information is required for the investigators to
17 do that kind of work, it would never pertain to
18 PII, but again I'm not one of those
19 investigators, so not best suited to be able to
20 tell you exactly the nature of, you know, how
21 some of those investigations potentially
22 develop.

23 MR. GRATL: Madam Registrar, could you please remove
24 the screenshot. Thank you kindly.

25 Q The information derived from the users of

1 Chainalysis Reactor software is used in part by
2 Chainalysis to ascribe risk; is that correct?

3 A Yes.

4 Q Right. So that's not open source information.
5 That's information derived from your client's
6 use of the software; right?

7 A No. Not necessarily, no. In relation to how we
8 attribute and identify risk, there's a number of
9 different ways in which that's identified. You
10 know, we talked today about the red flags and
11 typologies. For example documentation that FATF
12 produced, there are different kinds of
13 identifiers that exist for how we would qualify
14 something that's potential risky, running those
15 qualifications against data would then identify
16 potential risk.

17 Q All right. Sure, potential risk, then. But you
18 identify potential risk or ascribe potential
19 risk using in part the user log information;
20 right?

21 A We would do it based on-the transactions, based
22 on transactions, the transaction history and
23 what the interaction is with potential risky
24 activity.

25 Q Sure. But part of what you use in order to

1 assess that is the user log information; right?

2 A When you say "user log information," can you
3 define what you mean by that.

4 Q Well, I mean that your software generates a log
5 of all activities undertaken by your clients in
6 the course of using your database or accessing
7 your database?

8 A I think we do -- I mean, I think within the
9 software you saw I think that kind of log is
10 generated. I don't know what the scope of that
11 log is, right, in relation to what that looks
12 like, but we do obviously have that kind of
13 information, yes.

14 Q But your user agreement require that the user
15 log information becomes the proprietary
16 information of chain analysis; right?

17 A I think that not all of our user agreements are
18 the same. I think some of them require certain
19 information. I think other contracts that we
20 have have different requirements, so I don't
21 think anything would be universal, no.

22 Q So I didn't say it's universal. So for some
23 users, then, you're saying yes, the user log
24 information becomes proprietary to chain
25 analysis?

1 A I have no idea, again because I'm not in
2 contracting. I'm not in sales. I'm not in any
3 of that kind of engagement. So a lot of the
4 questions that you're asking, unfortunately, I
5 am not best suited to answer. I'm sure that's
6 frustrating and I apologize.

7 Q It is what it is. The risk information then is
8 not just derived from the blockchain and from
9 the register of transactions. There are other
10 sources, some open sources, some proprietary to
11 you and some purchased from other sources. Is
12 that right?

13 A I don't know if I would say purchased from other
14 sources in relation to how we identify risk. I
15 don't know if I would include that. I do know
16 that we do do some proprietary analysis, we rely
17 on specific regulation that has come out, you
18 know, regulatory specifics. We rely on the
19 data, the attributions that we've made. There's
20 a number of different components that are
21 associated with that.

22 Q I just note that in your "2020 State of
23 Cryptocrime," tax evasion is not included.

24 A So I would encourage you -- it's funny you
25 should say that, sir. I would encourage you

1 next week to tune in. I am doing a session we
2 call Links, which is our virtual event series,
3 with two of the J5 chiefs that specifically
4 focus on tax evasion, tax avoidance, in relation
5 to cryptoccrime in part. I've done a lot of work
6 and executed some of the first successful cases,
7 and certainly that is a focus area as well that,
8 you know, we have an appetite for and that we
9 work in as well. I think one of the things that
10 you raised which is important and interesting,
11 right, is until you have further regulatory
12 scrutiny around tax in this space, data can only
13 be contributed and built by way of
14 investigations and other information, and I
15 think tax laws and as that pertains to
16 cryptocurrency is something that's still
17 developing around the globe. But certainly not
18 something that was, you know, an oversight on
19 our part. I just think it's a developing kind
20 of category in relation to illicit activity.

21 Q Is it fair to say, though, that Chainalysis
22 treats large institutional investors as a sign
23 that cryptocurrency is achieving legitimacy
24 rather than a potential source of crime itself?

25 A I think that we treat our customers and any

1 entities based on the activity that we see on
2 chain and the risk that we're able to identify.
3 We have customers that have had illicit activity
4 associated. We have called that out before. We
5 have identified that. So it's all based on
6 applicability and the kind of data that we have
7 for how we're able to make any kinds of
8 determinations.

9 Q What would you recommend as a policy
10 prescription to stop money laundering on the
11 part of large institutions?

12 A That's a juicy question.

13 Q It is. It's an interesting question and one
14 that your reports don't seem to engage with
15 directly. And quite the opposite. Your reports
16 seem to suggest that large institutional
17 transactions are a good thing for crypto and a
18 sign that crime is on the wane rather than
19 waxing, blossoming. Isn't --

20 A I think that the question --

21 Q Sorry.

22 A No, I think the question is predicated on what
23 is defined and determined to be illicit
24 activity. I think it's very difficult given the
25 kind of information that we have access to, what

1 we've been able to develop, to make those kinds
2 of determinations based on what currently exists
3 and the laws that currently exist in relation to
4 the kind of data and determinations and
5 assumptions we could potentially make.

6 Q Well, you've got gambling, sextortion, phishing
7 scams, Ponzi schemes and things like that in
8 your list of illicit activity, and that type of
9 activity is used to build what you call the
10 typologies of crime and build groups such as the
11 Rogue 100 set out in your report. But I don't
12 see any reference to crimes committed by large
13 institutions like bread price fixing
14 transactions or diversion of pharmaceutical
15 opiates or bribery of public officials.

16 A Yeah, I mean, if there's a cryptocurrency nexus
17 directly that can be attributed to any of those
18 kinds of cases or activity that is something
19 that with we qualify. I think that falls
20 outside of what we see traditionally in the
21 cryptospace and the kind of determinations that
22 we can make. I referenced earlier in this
23 testimony, and this is an important distinction,
24 in relation to activity that happens offchain,
25 right, we don't have visibility into that,

1 right, in relation to the actual blockchain
2 information and history. If one of those
3 institutions that you're talking about gets
4 charged, right, huge civil penalty. Something
5 big comes out, they get hammered, and there's a
6 nexus with crypto. There is a potential impact
7 there depending upon what that nexus with crypto
8 is and what their interaction is with the
9 ecosystem. So, you know, that's kind of my
10 response --

11 Q But you --

12 THE COMMISSIONER: Sorry, I think the witness was --
13 hadn't completed his answer yet, Mr. Gratl.

14 MR. GRATL:

15 Q Sorry. Go ahead. Sorry for interrupting.

16 A I was finished.

17 Q I thought you were done your answer.

18 A I was. No, no, no, I was just saying it's very
19 hard. What we're usually doing is there's some
20 kind of fairly linear connection. So this is
21 going way out in left field and trying to make
22 that potential connection based on a lot of
23 speculation, and I don't say that outside of the
24 fact that unless you can provide me tangible
25 evidence where big financial institutions or

1 other are directly engaged in this kind of
2 activity in the cryptocurrency ecosystem. If
3 you can provide that I would love to see it
4 because, again, we are white hats. We're trying
5 to make this a clean ecosystem. I just don't
6 know of it.

7 Q Do you monitor the crimes committed by large
8 financial institutions?

9 A So I've done a lot of work with Transparency
10 International. I used to head up the
11 World-Check product line when I was with both
12 Thomson Reuters and Refintiv. I'm intimately
13 familiar with illicit activity that has occurred
14 as a result of a myriad of different kinds of
15 activity executed by large financial
16 institutions. I teach a number of courses for
17 the Association of Certified Anti-Money
18 Laundering Specialists in relation to large
19 financial institutions. In short what I'm
20 saying is I am intimately familiar. I could
21 tell you about any of the big banks from BNP
22 Parabas to Wells Fargo, all the different kinds
23 of initiatives that have occurred historically,
24 legacy, the different kinds of information
25 sharing relationships that now exist as a

1 result, specifically and explicitly, of
2 different kinds of illicit activity. I
3 personally am certainly aware of that kind of
4 activity and things that we've seen in the past.
5 But again, we're talking about virtual assets
6 right now, and the interconnectivity, it feels
7 like this is a bit of a reach to try and make
8 that connection.

9 Q Well, in Canada, for example, we have Scotiabank
10 was involved in handling bribes for a large
11 infrastructure project in Costa Rica and the
12 engineering firm SNC-Lavalin recently accepted
13 its responsibility for infrastructure bribes for
14 the son of Muammar Gaddafi in Libya. Does that
15 kind of information get added to your database
16 as an alert for companies that engage in
17 criminal activity?

18 A Do our database, no, because our database is
19 filled with companies and entities that are,
20 again, within the virtual asset space. If one
21 of those companies that you just mentioned, if
22 that company that you just mentioned were
23 entering into the cryptocurrency ecosystem or
24 was in the cryptocurrency ecosystem, that
25 information would certainly potentially be

1 relevant; right? Might surface. But again
2 we're talking about a specific ecosystem; right?

3 Q Sure. But do you as a company prevent those
4 types of large institutions that have been
5 convicted of serious regulatory offences or
6 crimes from accessing your ecosystem, your data
7 set?

8 A Well, any of the large financial entities that
9 you just referenced and I just referenced have
10 not been shut down. They've usually faced civil
11 enforcement penalties, corrective actions, for
12 example. They're still in operation.
13 Additionally if you look at the scope of the
14 illicit activity, comparatively to the entirety
15 of the activity, you know -- actually, forget
16 that last part. Scope, right. Any illicit
17 activity is bad illicit activity, and I do
18 believe that wholeheartedly, but if they faced
19 civil action, if they're still in operation if
20 they've taken corrective measures, if those
21 kinds of things have happened, I would be
22 curious to know why you would then try to deny
23 access to more financial inclusion banking or
24 services, which is again based on the concept of
25 institutional adoption something that, you know,

1 I think we encourage.

2 Q I'm concerned that the way your database is
3 structured and the way your alerts are
4 constructed and the way illicit activity is
5 constructed the services you provide contribute
6 to the selective enforcement of money laundering
7 laws?

8 A I would not think that there's any selective
9 enforcement. I think there have been
10 deficiencies that have specifically been
11 identified for a number of years that were
12 identified in relation to the virtual asset
13 ecosystem and that we're providing support and
14 services to build more financial integrity in
15 the cryptocurrency space. And as more
16 institutional adoption does occur, because it is
17 relatively limited to be clear right now
18 although developing, then there is other
19 potential information, specific risks that could
20 potentially be identified, et cetera. Right?
21 But as of right now there's disparity, I would
22 say, and it's not interconnected like is
23 potentially being proposed. On the illicit.

24 Q I'm being told that I'm out of time.

25 A I have to tell you something, I loved working

1 with Transparency International. I think you do
2 fantastic work and I just would like to say
3 that.

4 THE COMMISSIONER: All right. Thank you then.

5 MR. GRATL: Thank you kindly.

6 THE COMMISSIONER: Thank you, Mr. Gratl. Is there
7 anything arising as far as you're concerned,
8 Ms. Magonet?

9 MS. MAGONET: Nothing arising, Mr. Commissioner, but
10 I wanted to mention that I failed to ask you
11 earlier if we could have the PDF from the
12 Chainalysis website marked as an exhibit.

13 THE COMMISSIONER: Yes, I think we're at exhibit 160
14 now.

15 THE REGISTRAR: 260.

16 THE COMMISSIONER: 260. I'm only out by a hundred.

17 **EXHIBIT 260: Chainalysis Reactor webpage**

18 THE COMMISSIONER: All right. Thank you. Ms.
19 Chewka.

20 MS. CHEWKA: Nothing from me, Mr. Commissioner.

21 THE COMMISSIONER: Thank you. Ms. Rose.

22 MS. ROSE: No further questions for me,
23 Mr. Commissioner.

24 THE COMMISSIONER: All right. Thank you. Thank you,
25 Mr. Spiro, and you're excused now from any

1 further testimony. Thank you for your time.

2 **(WITNESS EXCUSED)**

3 THE COMMISSIONER: Ms. Rose, I haven't heard from any
4 of the participants whether or not they require
5 Mr. Place. Is that something you wish to deal
6 with them on offline or is that something we
7 could profitably deal with at this point?

8 MS. ROSE: I might suggest for efficiency's sake that
9 we have participants if there are any further
10 concerns arising from this say so now on the
11 record.

12 THE COMMISSIONER: Right. Ms. Chewka.

13 MS. CHEWKA: No, nothing from me, Mr. Commissioner.

14 THE COMMISSIONER: Ms. Magonet?

15 MS. MAGONET: Nothing from me, thank you.

16 THE COMMISSIONER: And Mr. Gratl?

17 MR. GRATL: Yes, Mr. Commissioner, I do have some
18 remaining questions of a technical nature
19 dealing with --

20 THE COMMISSIONER: I'm sorry, you're breaking up.
21 Sorry, Mr. Gratl, you're breaking up on me.

22 MS. ROSE: I wonder if it might be preferable in
23 light of the ...

24 MR. GRATL: Is that any better, Mr. Commissioner?

25 THE COMMISSIONER: Yes, it is. Thank you. Yes,

1 thank you.

2 MR. GRATL: Subject to your being interested in
3 further exploration of the topic,
4 Mr. Commissioner, I'd like to ask further
5 questions about the sources of information used
6 by Chainalysis to generate its list of illicit
7 transactions and Rogue 100 and so forth in
8 service of the larger notion that large
9 institutional actors, including Canadian banks,
10 are effectively insulated by the structure or
11 the architecture of the Chainalysis Reactor
12 software from scrutiny.

13 THE COMMISSIONER: Okay. Ms. Rose, do you have a
14 position on that?

15 MS. ROSE: I do have some concerns with respect to
16 those questions, Mr. Commissioner. In my view
17 Mr. Gratl has explored this area with Mr. Spiro
18 already. And I'm not clear how those questions
19 would be within either of the witnesses'
20 expertise here today based on the CVs tendered
21 as evidence. But I do wonder if we might want
22 to deal with these issues offline and see if
23 there's a resolution that might be available
24 with Mr. Gratl.

25 THE COMMISSIONER: Okay. Yeah, I don't want to

1 unnecessarily curtail his quest for cogent
2 information. I do however remind everyone that
3 we're concerned with the problem of money
4 laundering in British Columbia, and that as I
5 understand it this portion of the evidence is
6 devoted to exploring the issue of the risks that
7 are associated with the development and
8 evolution of virtual currencies. Certainly the
9 question of whether or not large institutions
10 are involved in money laundering is potentially
11 a question of interest. I'm not sure whether it
12 intersects with these witnesses' evidence or
13 not, but I'm perhaps a little unclear,
14 Mr. Gratl, on what it is you're driving at. So
15 maybe it's a good idea to discuss it offline
16 with Ms. Rose and see if you can arrive at some
17 accommodation. All right?

18 MR. GRATL: Thank you, Mr. Commissioner.

19 THE COMMISSIONER: Thank you. We will adjourn, then,
20 until tomorrow at 9:30 unless there's something
21 else to deal with, Ms. Rose or Mr. Martland.

22 MS. ROSE: Nothing further from my end, thank you,
23 Mr. Commissioner.

24 THE COMMISSIONER: All right. Thank you. Tomorrow
25 at 9:30 then.

1 THE REGISTRAR: The hearing is adjourned until
2 November 25th, 2020 at 9:30 a.m. Thank you.
3 **(PROCEEDINGS ADJOURNED AT 1:36 P.M. TO NOVEMBER 25,**
4 **2020)**

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