Thomson Reuters market insights.
A podcast for tax, legal and compliance professionals around the globe.

Episode title: Cryptocurrencies and the future of American security

Release date: November 17, 2021

Gina Jurva: Hello and thank you for joining us today for our Thomson Reuters Market Insights podcast. My name is Gina Jurva, Attorney and Manager of Market Insights and Thought Leadership here at the Thomson Reuters Institute for our corporate and government businesses. Today we have a special episode dedicated to our upcoming Thought Leadership conference in Washington DC on December 2nd, titled '"Those Darkest Hours": The Future of American Security'. It's a full day conference dedicated to public private partnerships combating domestic terrorism, managing social media and disinformation and the evolving illicit finance threat environment. Well, joining me today is Jose Caldera, Chief Product Officer at Acuant, an AI powered identity platform providing identity verification, regulatory compliance and digital identities solutions. Jose is also a panelist on the upcoming illicit finance panel. Jose, thank you for being here.

Jose Caldera: Oh, thank you so much for having me here, Gina, always a pleasure talking with you.

Gina Jurva: It's always a pleasure talking with you. I think, the probably the best way to start this is really with some level setting for those in the audience who aren't as familiar with just how the illicit finance threat environment is, how bad it is. Can you give us some just overview of this ecosystem?

Jose Caldera: Sure, you know it is sort of calculated that we lose somewhere between 2 to the 5% of the overall GDP in illicit activities associated, you know, with money laundering. And there is obviously billions and billions of dollars that are lost yearly to fraud and that in some cases may be related to money laundering, some other cases may not, but the whole spectrum of financial crime in how our ecosystem and financial ecosystem is being abused by criminals is actually pretty extensive when you think about the amount of trillions of dollars that accounts to write that in and we still don't have visibility fully or we suspect we don't, we as an industry, as law enforcement, we don't have this ability to about 90% of what really goes, but you know every so often when you get things like, you know, the Panama Papers or Pandora Papers, you start seeing how money moves in, how bad the issue is, and how important or relevant it is for us all to be part of trying to protect the financial system.

Gina Jurva: That's such a great point that the Pandora Papers just highlights it and, you know, what you said, 90%, we may not even know. 90% of the amount of illicit funds flowing through financial institutions we might not even be catching. So, the number I have heard the same thing that the numbers in, you know, the trillions. Some people say hundreds of billions like it's just, it's hard to really put an accurate estimate on, but we know it's a problem, so that's, you know, that's I think why we're going to be having this conference to really talk about it. What about you know the buzzword and so much of even just what I read in the in the daily newspaper is cryptocurrency, virtual currencies I talked to so many so many folks in the industry about virtual currencies and the Biden administration clearly has taken a stance on it. How are - again just kind of level study - how are virtual currencies being used by bad actors?

Jose Caldera: Similar to cash in a way, you know, crypto offers some level of anonymity, right? So, once you have a virtual currency, that virtual currency you own, that virtual currency, right? There is no attachment so you can use that coin and whatever you can. And in blockchains and in the way that they work, they work to provide such a level of anonymity to who is the person that is transacting, however, because all of these transactions get registered into blockchains, which is, you know, the sort of the online by [inaudible] of how money moves it actually is in a way it's a lot easier to track cryptocurrencies than is to track other things like cash for example, where you don't where you really have a record of who moved that money to something else, right? So, I think that outside the hype and outside the media focus on everything, I still think that it's a lot in my mind, there's a lot of tools inside the crypto world that allows us to look at things and how they are being used that are actually better than the traditional financial ecosystem. So, but there's still - there's no question that there is a section of actors are taking that technology and they are using it for nefarious purposes, and there are certain types of coins and infrastructure that makes it even harder, right? So, we have these concepts of tumblers or we have these concepts of chain hopping where you tried really to hide where you make your transactions and how they go from one coin to another and then to another and then to another right? So, there are ways that the financial ecosystem is used to get payments, but by large then it's really about, you know the fundamental concept of the technology that allows for certain level of anonymity in the transaction, but again I still think that, you know, we just haven't gotten used to it because I say the infrastructure I think is going to get as much more information actually than in the rest of the financial ecosystem.

Gina Jurva: Not as anonymous as we as we think it is, right? Like there are ways, even though it's the record, the transactions on the blockchain, there are ways to figure out to kind of back extrapolate the identity of the user, especially in, again, these cyber-attacks.

Jose Caldera: Well, yes and no. So, it's easy to - well, I wouldn't say it's easy but there is the technology allows you to track how the money moved in a way through the infrastructure, right? And I think that is in my mind that is far easier to do than in the financial ecosystem, in the traditional financial ecosystem. Now, in order to associate a particular currency to a particular user that's when things start becoming a little more difficult, right? Because every transaction that you make is not necessarily associated with a name or a, you know, a particular user or individual. Part of the regulatory framework, right, is trying to get this, and this could be the digital currency exchanges, or it could be the LDC's right that that are being regulated, regulated in a way that they are forcing those parts of the infrastructure to go through a for the users of those controls would go through a KYC process. So, if you are an exchange and it's a currency exchange and you are in a jurisdiction where exchanges are regulated, then those exchanges or those brokers are going to have a full KYC process where that allows you to is that you associate a name and a user, or an individual or a business entity to basically a wallet inside that exchange and then add those exchanges that you can track who are the owners of the wallets where the money is moving from and to, that is. With the adoption of the travel rule and enforcement of the travel rule and that is actually going to step beyond staking serve from the from the wire mechanism in the traditional ecosystem where you have to, where you have as provider of moving the money. Now you need to provide information not only about where the transaction is coming from, but also where it's going into, right? So, it's you have sort of to keep information about both ends at that, so but not every part of the infrastructure is regulated, right or exists in a country where that is regulated. In that case then you don't have that connection, you don't have that connectivity between the user and the transaction itself on the coins that are being monitored. So, there are parts then where there is much more visibility than

other parts where you don't have that level of visibility and you know in the cases of the colonial pipeline where the, you know, the FBI was able to recuperate, you know, about half of the money that was paid. What ends up happening is that one of the exchanges were those currency was stored at was being regulated and the FBI had access to it right? And then in those cases that you can see, and you can, you can get access to most information, but if you think about, you know, recently consent in the OFAC, putting the sanctions list, for example, a broker that was in Russia, right? and the regulatory framework in Russia is still not very clear when he comes to brokers or he comes to exchanges. There is a law there that was supposed to happen at the beginning of this year, but it's going to happen at the beginning of next year and until those regulatory frameworks are put in place together, then there's little visibility that governments can have about in these infrastructures. So anyway, so the point being here is that the infrastructure if has the tools to associate users to some of those transactions, the visibility that the law enforcement has on that is limited again because of the global decision, right? So, you could choose to move your money into coins or into pieces of infrastructure where there's little visibility into it and the other thing is also true, right? So, the same way that you, you know, that you do is structuring in in the wall of money laundering where you hide, you know, yourself or you hide the money behind shell companies and support, there's a very similar concept in going on in the virtual currency infrastructure where you can move the money through multiple exchanges very fast and then that tends and then use different mechanisms like tumblers and so forth, so that you start hiding where the currency went through right? So, you know, it's kind of like an old type of scheme that is being adapted to the new infrastructure and the passage of the new infrastructure.

Gina Jurva: Yeah, and you're right and it's like it's like that fat phrase everything old is new again. I mean I, I think, you know, trying to find ways to layer the transactions and doing it through different crypto exchanges or tumblers like you said is, is a lot of what we're seeing in the environment right now. And I think further, not to put too fine a point on it, but as the Biden administration and the Department of Justice are working on this, I think it was earlier in October that they announced the establishment of a national cryptocurrency team to assist with tracing and recovering assets lost to things like fraud and extortion. I mean, just how difficult is it to recover assets lost to these types of crimes? I mean, trying to claw that money back after it's gone. And we did see it in the colonial pipeline, as you mentioned. But what is the difficulty level for this and why?

Jose Caldera: Well, it's difficult at the moment and it's hard to tell at the moment, you know, it hurts at the moment because we are still not used to it, so our law enforcement is not used to it. I think that if we track how the money from the colonial pipeline was recovered it gives you a lot of hope because there is, as I said before there, there is a lot of capabilities in how you can track transactions and how you can figure out where that money is sitting at and if where he's sitting at is in the scope of your jurisdiction or it's possible, right? And it's exactly in a way what happened with the colonial pipeline. So, I think that gives you some level of hope that you can actually retrieve that. The other aspect of it is that if that money is converted into Fiat currency, right, then the outputs in the “off roads”, if you will, between the virtual currencies and the liquidity in terms of local currency. Those tend to happen in or those seem to be happening in regulatory environments where there are regulatory frameworks that are going to look at, you know, source of funds and you have to justify these things so there is a possibility that as they become part of the traditional financial, then law enforcement knows how to do that much better and much easier than within the crypto world, but if it remains in the crypto world and it could be difficult, right? Because at some point that crypto can be held, you know the same way as

cash, right? You could stash it under the under whatever you want, right? So, you could get those wallets to be completely independent, so I could install software that maintains my cryptocurrency without having to expose it anywhere, right? So, I think that there are different avenues and I think that in my mind, again, I continue to say to me that this will be easier than cash, right? But it requires law enforcement to be better trained to understand better the ecosystem and so forth. And I think it's going to happen. I mean, as we get more nefarious activities with such visibility, right? Then the government is going to act as it happens and INCET, the National cryptocurrency team that you are referring to, I mean, we're talking about weeks in the making, right? So, this was announced, what two weeks ago? Week ago, or something like that? And if you think about that, about a year ago was when we got the if we think about the DOJ put together that and LARS, right? That was a year ago that wasn't like, you know, we're talking decades. We're talking a year ago. And then so, that LARS from DOJ is really focused on how you recover money from money laundering, right? So, a year later you get the cryptocurrency added to this with the INCET team that is leveraging the same infrastructure. So, I think we are just getting ourselves trained and prepared to how we're going to accomplish these things, and I said, I think, that what we did or what was done with the current pipeline, I think is a good example and it gives us hope that we're going to get to that point where it's not as difficult to retrieve the money form from financial crime.

Gina Jurva: Yeah, and I think it, as we said, it's still only a fraction of the money that's being monitored or used through via cryptocurrencies. I think it's, but some of the stories that come out of I was talking to a member of the IRS criminal investigations yesterday. Talking about how terrorist organizations, when they are sourcing funds for their own activities, their terrorist activities, they used cryptocurrencies and they had several examples of that. So, it's interesting to keep following this and seeing how law enforcement is paying attention, as you said, how the regulations are different throughout the world. Global regulations are constantly changing, and I think we're still all trying to get a grip on it. And I think that's even more acute when we talk about, as you said, KYC, knowing your customer laws, requiring financial institutions to verify a customer's identity when doing business, you know, traditional financial institutions. With crypto exchanges you mentioned earlier that that happens in some manner, so like I think Coinbase is a good example, right? But how would having strong KYC requirements really help stem the flow of illicit finance or illicit money laundering going via cryptocurrencies and allowing the actors to survive and, again not to put too fine a point on it, but how would you- how do you see that these KYC requirements could really help stop this? I mean, knowing your customer?

Jose Caldera: Well, it, you know, if you think about that the exchange of currencies, right? At some point, so again, the majority of cryptocurrency moves through exchanges in the world, right? So, that infrastructure, you know, I can move cryptocurrency directly to you without having to go to an exchange, but at some point, I have to have gotten that currency. So, unless you are in the world of mining, where'd you get rewarded directly to your wallet, or you could get reorganize their wallet for mining, in most cases right at some point to acquire that virtual currency you likely went through one of these exchanges where you're able to exchange the said currency into crypto. So, if we're able to, you know, to penetrate the infrastructure and to make sure that we understand who is everyone that is putting the money and buying the currencies and exchanging the currencies you know sensibly, then then you have the ability then to connect, you know, each currency to a particular user at any particular point in time, right? Which is something that you cannot do if you think about it, that's something you

cannot do with cash, for example, right? So, there is a potential value here that is in infrastructure. Now having said that, most obviously, you know, my view in the world of exchange is a little bit skewed because I work with exchanges and I've been working with exchanges now for almost, you know, since 2013 when Bitcoin became mainstream. And most of my clients are exchanges or the one under the right thing, right? We don't see those exchanges. For example, those brokers that don't do KYC, right? And there are many, many, and in part because they are in jurisdictions where the regulatory framework is not very clear or it's not very strict. Or just because they are created from terrorist activities you know directly, right? So, my view of the world of crypto is bias heavily to the right people and the people that are you know that have a career out of being a compliance officers and they want to do the right thing and they are very worried about their infrastructure being utilized for notorious activities and they keep real strong programs of anti-money laundering, where KYC is part of that. So, ostensibly, you know, you have all the all the frameworks and all the different things and then they are making sure that they know who their customers are and when transactions are higher or the users consider higher risk than they do proper enhanced due diligence on those clients, and so there is a fantastic effort in to get that done. So, if you do that well then you have a better chance of understanding who moved the money from one place to the other. Now unfortunately, then there there's the problem of, you know, the identity theft, right? And how you create identities that that are created for the purposes of doing the various activities. So, then that part is hard, right? So that that point is no longer necessarily chose to do a KYC, right? You have to understand now that these identities are being used online, could be fabricated, could be or it could be stolen from good people, right? And sometimes that that process you have to go deeper and deeper and deeper. So, it's not just you know making sure you do KYC. It is making sure that you're able to beef up that those processes so you can detect synthetic identities or stolen identities and so forth, right? So, the process of KYC that push for KYC has to be deeper and deeper and deeper and not every organization has the focus or has the resources to implement processes that are that that can be expensive when you when you're trying to really weight down, we will forget, right? So, 99% of the transactions are good transactions. It's just that 1% that you have to be, you know, and you have to invest a lot of money to identify that 1%. So, the good news though, is that there's technology, right? So, I do think that the technology has become better and it's providing better tools and it's providing you know more possibilities and more access to different types of sources of data to detect to detect this identity related issues, but again, it's it you know when you go that route, you're pushing those providers of financial services including the crypto exchanges. In this case you're pushing them to go all the way there and implement all these technologies and in different cases and implemented good risk-based approach and so forth such that this the burden of the cost of this becomes effective, right? Otherwise, you know, you spend too much money. And then and then you know you still have to learn the business, right?

Gina Jurva: Right, well, it'll be interesting to see if you, for those that aren't aware, El Salvador recently adopted cryptocurrency as their as one of their legal tenders and they're the first country to do that. So, it'll be interesting to see how they manage this. I know so far, it's gone, rather bumpy for them. I think we should all pay attention to El Salvador and see how they work through it.

Jose Caldera: I think so too and I was going to say that that so, you know, Venezuela was one of the first countries in putting a or they called the Petro, which is also government issued crypto and there are there are valued and people are taking a good approach to it, so I think that we are just at the beginning of seeing how governments are going to use it. I do think that next year we're going to see something

from China coming into specifically issued cryptocurrencies as a legal tender in there and it seems that Russia is going to also move in that direction. And we know of countries in Africa that is going to move in that direction too. So, I think I think next year, you know, we will see some acceleration of adoption of cryptocurrencies from governments and that I think it's a reality. It's going to continue to evolve is going to continue to get more adapted, and it's going to get people are going to start understanding better how to use it, how to monitor it, but at the same time as you know, criminals have always done throughout our history, they will find ways of how you can take advantage of the financial ecosystem. Doesn't matter if it is traditional, doesn't matter if it is crypto, there are always going to be ways. We need to keep working with technology with the regulators with law enforcement and see how we can better protect our infrastructure.

Gina Jurva: That's very well said. I think, you know, final question here and it's really about Bitcoin itself, not to single that out. But earlier in October, since then issued a compliance guidance report and they did analysis of ransomware related suspicious activity reports those SARS that mentioned that acronym that banks file and this was during the first half of 2021. Bitcoin was found to be the most common ransomware-related payment method among the $590 million in ransomware related SARS filed during, like I said, the first six months of 2021. Is that surprising to you? Is there a reason Bitcoin would be the most common that you can think of?

Jose Caldera: Not surprised. I think that if you're tracking how valuable Bitcoin is, I think in how pervasive it is, you know, I'm talking pervasive within the crypto world, right? And I'm not surprised that Bitcoin would be given that is the, you know, the first and the most famous, virtual currency out there at that level, it's easier to get, you know to get Bitcoin than to get, I don't know Dutch coin, for example, right? So, I'm not surprised that that Bitcoin is, I'm not surprised either about, you know, the numbers, right? I think the same reports, I think Vincent was talking about 5 billion or a little bit north of 5 billion that there was tied to Bitcoin payments for ransomware, right? And overall, I think it's a matter of access and I think it's a matter of people understanding and knowing. So, if you are a criminal and you are, you are doing some form of ransomware and, you know, things that are, you know, fascinating and scary at the same time, right? So, there are services, ransomware as a service, I don't know if you know that, but it's kind of interesting that you could go and buy a service to perform ransom so you can go then do ransomware and in a tag via these services. So, the proliferation of that of those schemes, right? Then people want to is, like, you know, ways like using dollars, right? For money laundering, right? So, it's way easier and it's more valuable to use dollars and to use another other currency, right? Because the value maintains, the dollars are by far the currency that dominates the global market, so it's I think it’s just that is simply that Bitcoin is the most widely accepted currencies, that the currency that people know the most, is the one that continues to hold its value and continues to grow its value in the market. I'm not surprised.

Gina Jurva: Well yeah, that's I figured it had to do with, you know, accessibility and also, it's like Bitcoin is quite the name recognition too I think when we think of cryptocurrency that typically comes up as our first thought. But no, that that makes sense. I guess any final thoughts we'd like to leave the audience with before the big conference coming up in December. I mean, is any final thoughts on the identity verification? And really how important it is in income combating financial crime?

Jose Caldera: Yeah, you know it's obviously that's my day today, right? I think that that identity is the way to make sure that you as a business or some financial provider as a, you know, part of the financial

ecosystem, understanding who your users are in understanding what makes them a good user. It's just fundamental. It's not just about whether Jose, you know, has a proper driver's license or a passport. It's about Jose's behaviors, right? It's about how it's performing in the in the financial ecosystem or in the payment ecosystem and so forth. So, it's the knowledge, right? The amount of information that you, as a provider of servants, have about a particular user and how to use that information such that you can do better monitoring, a better understanding of its fundamental and people are, you know, are afraid of privacies and privacy laws and so forth. And I think all of those are, you know, are valid concerns and, and, you know, technology exists in so many different ways that can help you do good analysis of individuals and business entities without having to expose or having to, you know, to put in jeopardy the privacy of those individuals. There is, you know, and of course, being a vendor or provider technology, you know, to me this is this is this is the most important part, right? How we protect the individual's privacy and how we provide technologies that help our clients, you know, get to an actual understanding of those identities and at the same time protect their information right? So, to me, that that's where it all starts. And when I think about, you know, transaction monitoring and I think about, you know, identity theft and all those things, I think that the framework of understanding and the framework of capable technology that exists in the market today I think it's achievable. I do think so, and I think that the more you understand your customers, the more you understand your users and their identities and how they behave the easier it is to apply policies that are, you know, corresponding to the risk levels that you are at.

Gina Jurva: Well, thank you so much. A very, very important conversation. We will continue that conversation in walk in the Washington DC area, December 2nd Jose Caldera, chief Product Officer at Acuant. Do not miss your chance to meet Jose if you are in the DC area. The conference is called '" Those Darkest Hours": The future of American Security' please go to www.thomsonreuters.com/institute to register. Jose, Thank you so much.

Jose Caldera: Thank you so much, Gina. Always a pleasure.

Outro: Thank you for joining us, for Thomson Reuters Market Insights. For more data driven analysis of today's professional services market and in-depth conversations with industry thought leaders, please visit us online at thomsonreuters.com/institute. You can subscribe to this podcast on your favorite podcast platform or follow us on Twitter @TRIExecutives and LinkedIn under the Thomson Reuters Institute. Thomson Reuters Market Insights is a production of Thomson Reuters.