HOMELAND SECURITY EXPERTS GROUP (HSEG)

2021 HOMELAND SECURITY ENTERPRISE FORUM

PLENARY SESSION 8:

CRYPTO CURRENCIES AND RANSOMWARE

WITH DANTE DISPARTE, KRISTINA LITTMAN AND GEORGIA QUINN

Salamander Resort

Middleburg, Virginia

Tuesday, September 14, 2021

Plenary Session 8:

Crypto Currencies and Ransomware

MR. CLARK: There we go. Okay, good afternoon, and welcome to the single greatest plenary session of this 2021 Homeland Security Enterprise Forum.

(Applause)

MR. CLARK: I hope I didn't overhype it, did I? Anyway, my name is --

UNIDENTIFIED SPEAKER: (Cross talk).

MR. CLARK: That's right. The bar is high. My name is Rob Clark and I lead our Department of Homeland Security practice at TransUnion. And TransUnion is very proud to introduce this panel and our work with DHS on a number of important issues. And none such important issues as ransomware and cryptocurrency. If you're following the news at all, you've seen the high spike in ransomware attacks on the U.S. from critical infrastructure, obviously, the Colonial Pipeline incident, to healthcare to everything in between. And at the same time, cryptocurrency is

becoming a more legitimate form of -- part of our economy.

So, this next panel is going to talk about the intersection of these two important trends. And again, it's my great honor to introduce Juan Zarate.

(Laughter)

MR. CLARK: I messed him up. Zarate. Incredible man. A lot of great accomplishments, number one, proud HSEG member, right? But of course, he was the Deputy Secretary, Deputy National Security Advisor from 2005 to 2009. He's an author. He's the current global co-managing partner of K2 Integrity. It's going to be a fantastic discussion. Thank you so much. Let's give it up for, Juan. Juan, thank you very much.

MR. ZARATE: Thank you, Rob.

(Applause)

MR. ZARATE: Rob, thank you very much. Appreciate the heightened expectations for the panel, always appropriate. But let me start first by thanking you Rob, for the great introduction. Rob Walker, you and the entire team here, I'm honored to be a part of the HSEG group. Jane, your leadership, Michael

Chertoff's leadership, thank you.

I can't tell you how refreshing it is to be in the same room with friends, colleagues, new friends. There's a lot of energy, great ideas. And I'm proud to be moderating this session, hopefully adding to the ideas into the introspection as to where we are with the Homeland Security Enterprise.

When Rob and the team were putting this conference and forum together, we thought it had to be a panel on a discussion, where we talk not just about ransomware, which we've heard a bit about throughout the conference and throughout the forum, but the intersection between the rise of ransomware and cryptocurrency.

And as Rob mentioned in the introduction, the intersection of both the increase in volume in ransomware attacks, according to chain analysis, an increase of about 350 percent over the last year in the number of attacks, hundreds of millions of dollars in Bitcoin or crypto paid as a result. But meanwhile, the legitimation and the increase in the crypto economy, where the crypto economy is now clearly a part of the

financial system in various ways. And so, we wanted to put this panel together to enlighten as to what's happening at that intersection, and how to think about both the opportunities and the risks and vulnerabilities.

And I'm honored to be on this panel and moderating this panel with three great professionals who touch this environment in different ways. And I think you're going to see and understand the different perspectives.

Two of the panelists are joining us via video. So, welcome to Christie Littman, who is the Chief of Cyber Security at the SEC, the Division of Enforcement. Christie is responsible as a regulator for cyber security for the SEC. So, you can imagine all of those responsibilities. But she's also watching very carefully the crypto economy and the SEC, obviously has something to say about the regulation of the crypto markets.

We also have Georgia Quinn, who is the General Counsel of Anchorage Digital, sometimes known as Anchorage Bank for good reason, because in January of

this year, Anchorage was afforded the first license as a National Trust Bank by the OCC to be able to house and service crypto. And so, they are a crypto bank, if you will, able to service crypto assets. So, Georgia, welcome as well.

And last but not least, my compadre here on stage, Dante Disparte, who is the Chief Strategy Officer, Chief of Global -- Head of Global Policy for Circle. Those of you who follow the crypto industry, you know that Circle is one of the leading virtual asset service providers in the sector. In addition, they are the backer of USDC, the stablecoin, which is much in the news and much -- predominant in the marketplace, and also moving to become a registered and recognized bank.

So, we've got three great professionals who, on a daily basis, touch these issues and these risks, and we're going to talk to them about how they're seeing the environment. So, welcome to all of you.

Let me set the stage for just a second. Give me that prerogative. I've been very fortunate in my government career, I was a Senior Treasury Official,

Senior White House Official. In the private sector, I've been watching and working with the crypto industry very carefully since 2014. I've been an independent advisor to Coinbase, which made news this year going out with its IPO competitor, vast, but also a collaborative, vast competitor to Circle.

And what we see in the environment is not just the rise of ransomware. And as Chris Inglis said yesterday, two for the price of one cent of what ransomware now is, which is a source of profit and avarice for criminals, state, non-state actors alike, but also a source of national and Homeland Security, vulnerability, both putting at risk the confidence of our core systems, but also literally putting at risk, the accessibility of key infrastructure.

Colonial Pipeline struck, obviously, everyone's consciousness. It was very clear that ransomware was no longer just a business nuisance, no longer just this undercurrent of cyber threat that people were dealing with quietly. But now suddenly, emerged as something critical to our national and Homeland Security.

But with all that, we also know that crypto is not only a legitimate part of the financial system, it also enables ransomware. We know that ransomware is the malware that holds data or systems hostage from the owner, requiring then payment. And we know most of the payments in the ransomware context come in the form of crypto.

So, raises numbers -- a number of questions, additional questions about how we should think about the crypto environment with the rise of ransomware threats. And that's what we want to talk to you about today.

So, let's start first with Christie via her office at the SEC. Christie, if you could talk to us from your vantage point at the SEC as to how you view the ransomware threats? What are the threats that concern you? And what cases have you seen that the SEC has focused on in recent months?

MS. LITTMAN: Sure. Thank you. And thank you for that introduction. Sorry, I can't be there with you today. We are still in a mission-critical only travel status at the SEC. I also have to give my

standard disclaimer that that most government employees have to give when they're speaking at these events. The views I express today are my own. They do not necessarily reflect the views of the commissioner or the staff.

Back to the question at hand now. I think, you know, the thing that the SEC is most concerned about when we see ransomware attacks, or really any type of cyber security incident is typically around disclosure when we're talking about a public issuer.

So, public issuers obviously have obligations to provide certain disclosures to their investors. And they also have responsibilities to maintain internal accounting controls around their assets. And so that's another area that we look at. And we look at trading. So, we might look to see if it's a public issue or if there is a threat actor out there trading around the cyber incident, or if their internal company personnel that are trading around it. Obviously, when your company gets hit, you're trying to get your arms around it. Your IT folks often have a lot of information that maybe isn't available to the public yet and sometimes

we see trading, so we look at that.

But I would say for the folks here today, probably disclosure is the biggest area of concern for you, right? So, we're going to want you to make disclosure to your investors if you have experienced a material events, and you know, Juan kind of alluded to what some of the harms are that can range, or that can result from one of these incidents. It's not always just, you know, I think there are a lot of ways to kind of slice and dice whether something is material. But I think when you're making that assessment and deciding whether or not you have a material incident that needs to be disclosed, you need to look at the full range of harm. You know, it may be financial performance, but it may also be reputational or customer vendor relationships. It may be the type of event that results in litigation or regulatory consequences.

And so, you know, you should really be thinking about all of those when you're deciding whether or not you have something that needs to be disclosed. And we've brought a few cases recently that I think illustrate this.

The first is against a company called First American Financial Corporation. And that was -- this is a settled action. It's a real estate settlement services company, who had -- it wasn't a ransomware attack, but it was a cyber security vulnerability that exposed sensitive customer information and a journalist notified First American of the vulnerability, which had expose over 800 million images dating back to 2003, and including images with PII, social security numbers, financial information, things like that. And they issued a press statement, 8k to the commission in the following days. The issue that we had in this case was that the senior executives who were responsible for the public statements were not apprised of certain information that was relevant to their assessment of the company's disclosure and response to the vulnerability and the magnitude of the risk.

Specifically, the company had security personnel and the company had information about the vulnerability stuff several months earlier, and had failed to remediate this vulnerability and senior executives of the company were never informed of that.

So, when the journalist reached out and they made kind of reactive disclosures, they didn't have the relevant information about the kind of preexisting vulnerability that they'd had on their system for some time. So, we charged them with disclosure control violations and assessed a penalty.

Another example is a case that we brought this summer against a U.K.-based company that issues in the U.S. called Pearson. It was a London-based educational publishing company. And in that instance, again, we had a journalist reaching out to them, they had a 2018 cyber intrusion, where millions of student records had been exfiltrated, or had been accessed and included dates of birth and e-mail addresses. And when they were approached by the media, they had kind of a reactive media statement in the can already that they issued. But it turned out that that media statement was not quite fulsome and accurate. And so, our order found that it kind of essentially understated the nature and scope of the incident and overstated the company's data protections.

So, you know, the message there is just, you

know, when you are -- when you decide that you do have to make a disclosure to investors, you've got to make sure it's fulsome and accurate. In that case, it resulted in a negligent fraud charges, and a million dollar penalty was assessed there.

MR. ZARATE: Christie, let me weigh back in here. Because I think your point about disclosure is critical. I want to come back to this as we talk about the way forward, because I think one of the themes we've heard in the conference and Chris Inglis references is kind of the challenge of dealing with the government when the government's both the regulator and enabler, right, and how to think about that. So, I want to come back to that, given the cases you're referring to and others.

I want to turn to Dante now. Dante, I want you to give the audience a sense of how you see the crypto environment, how ransomware touches the world that you live in on a daily basis and how you think about that intersection of ransomware and crypto?

MR. DISPARTE: Sure. Well, thank you, Juan. And it's a really a great honor being amongst so many

Homeland Security leaders, especially during a time of solemnity and solidarity, marking 20 years since 9/11. So, I came at the crypto industry initially through a background of insurance, resilience, technology and national security. So, I've been sort of looking at the ransomware question, years before it became a thing. And in so many ways, I think right now just for level setting, and I'll answer the question also about what are the actors in the ecosystem. But in so many ways, I think the argument that crypto equals ransomware, smacks a little bit of convenience and it's missing the deeper vulnerability.

Correlation does not equal causality. More ransomware is triggered by e-mail, as the vector of attack and exploits that arise between the keyboard and the chair, then what method of payment may be used to settle a transaction to the extent the ransomware even has an economic motive in mind. So, we have to really start to correct what is today a very convenient clickbait sort of approach to telling a story. That is, you know, equating this scourge of ransomware with a means of payment on the internet, because millions of

options exist for how people might exact and extract financial rents, but not nearly enough time is spent asking and answering hard questions, which we of course, started in this conference about underlying cyber vulnerability.

And so, in the crypto industry, I actually think there's also a lot of the actors in the space are starting to normalize, what I'm characterizing as a blue checkmark moment, you see the exchanges, the digital asset service providers, the digital wallet providers, traditional financial services firms, whether they're Visa or MasterCard, and many other in between are actually leveraging this technology as a core upgrade to legacy financial systems, which are themselves vulnerable and themselves are falling prey increasingly to not only technological obsolescence, they're falling prey to a host of risks in their own right. And so, in so many ways, this novel 12 year old technology, blockchain and the financial innovations it's helping to underscore, represents the very type of national security resilience and economic competitiveness we have called for in the last day and

a half of this conference, and then putting that at the core of the financial system, not as competition, but as completing unfinished work. I think these are an important counter narrative to the argument that crypto equals ransomware. That's big point one. And I do think a lot of those actors are starting to coalesce around that.

The other very, very novel concept here is that unlike when you wrote treasuries war and when you helped lead -- I told you I would mention it.

MR. ZARATE: (Inaudible).

MR. DISPARTE: Unlike when you wrote treasuries war and you helped lead the post 9/11 financial crime compliance framework.

MR. ZARATE: I didn't ask him to do this, by the way.

MR. DISPARTE: I get a royalty every time I mention it on stage. The advent of public internet-based financial ledger's, blockchain technologies used for payments and finance is actually creating an ability to, I think, improve exponentially the types of gains we could have in combating illicit finance,

countering financing of terrorism, anti-money laundering and a whole host of big activities. The reason why is that if you wanted to launder billions and billions of dollars, you can call opaque, global, competitive banks using analog rails to do so. It's increasingly difficult and there's a lot of evidence -- and I suspect we'll get into it in the panel, it is increasingly difficult to leverage a public transaction that is internet available to anybody in the world to see, to conduct illicit activity and crime. It's a big counter narrative, but I often think these types of points are missed when you talk about crypto and ransomware.

MR. ZARATE: Well, to your point, you know, in the Colonial Pipeline case, we know that 75 bitcoins were paid, at the time about $4.4 million worth. DOJ after the announcement of the ransomware, about a month later, announced that they had clawed back 64 of those bitcoins, were able to track the wallet, seize it and pull it back. So, to your point, a degree of an ability to track and trace in a way that you might not otherwise be able to, for example, the cash drop or

something else in a conventional context.

The other thing that, Dante, I think you mentioned, which is important for the audience to notice, the emergence of a legitimate sector, right, that the crypto economy emerging as a legitimate part of the financial system requires legitimate actors, requires more regulation, requires enforcement, the type that Christie was talking about. And you have lots of regulators now looking at this and looking at ransomware. You have OFAC, FinCEN out with guidance, et cetera.

With that, I want to turn to Georgia. Georgia, you're the General Counsel of Anchorage Digital. So, you're right in the middle of dealing with federal banking regulators, looking at what regulators in the U.S. and around the world are asking for. You're also seeing the marketplace deal with ransomware. Can you talk to the audience about what you're seeing in the marketplace and frankly, what you worry about given your role as the GC for the first ever, you know, National Trust Bank dealing with crypto?

Georgia? I think you're on mute, Georgia.

MS. QUINN: Of course, I am.

(Laughter)

MS. QUINN: The first time I've done this. I'm so sorry about that, guys. Listen, I just wanted to thank you, Juan, for inviting me to this. This is such a great event. And Dante, I have to thank you for making that very important point of clarification and separating ransomware from cryptocurrency. They are two completely different things. Causation is not causality. And I'm so glad we're able to spread that message today.

When I think about how, you know, what we deal with, as a bank, we're really merging these two worlds of, you know, very highly regulated financial institution and cutting-edge technology, cryptocurrency space. Oftentimes, those things can be at odds. And I think when we look at ransomware and other types of, you know, nefarious activities, it really puts a very fine point on that. And one thing that we have experienced is traditional insurers and security firms that are, you know, have already been in this space,

where they insure against these types of bad acts, are looking to legitimize as we've been kind of saying, their procedures around how they actually have to ultimately go out paying out to these bad actors in, you know, some sort of payables sort of event. And they're looking to partner with, you know, financial institutions, or, frankly, you know, some party that can assist with, you know, both the custody and then the settlement of these types of payments, but then, of course, have the ability to continue to track and trace as was done with the Colonial Pipeline event, and, you know, ultimately, potentially prevent at least the loss event.

And so, we think about that, and that sounds like a great idea, right? Like, we would get to be superheroes and help, you know, spoil these bad actors plans. But then we think about the Bank Secrecy Act and our requirements as a federally regulated financial institution. And we know that we cannot engage in those types of activities, because they would violate all of our AML procedures, like we actually know that we are engaging in, you know, a bad act, and paying to

I'm sure, some, you know, probably sanctions individual. And we, you know, we'd like to think about -- and to go back to the just immediate panel that was before us, some type of public private partnership, potentially, to allow these regulated institutions to assist the government with these kinds of activities, this tracking and tracing as this type of activity is becoming more prevalent.

And then just to take it a step further, because, you know, we're not just talking about ransomware, we are talking about, you know, the full scope of national security. We'd like to implement the Bank Secrecy Act and these types of procedures throughout the cryptocurrency ecosystem. And we think this can only be done through, you know, obviously, these institutions embracing regulation, but also regulators embracing those institutions.

And we, you know, frankly, we think we need more federally regulated crypto banks, not less, even though that might be a bit detrimental to us from a competition standpoint, we actually think that in order for these regulations to properly function, they need

to have, you know, we need to have a network of these regulated institutions that can talk to one another, and, you know, transmit assets to one another, utilizing the full scope of the Bank Secrecy Act. We kind of call it the manifest destiny of the Bank Secrecy Act. And it really only works when you have a lot of institutions under the same regulatory umbrella.

MR. ZARATE: Georgia, thank you for that. And I think what you just described is the manifest destiny, the Bank Secrecy Act has been part of a broader debate in the, you know, financial regulatory world around stronger, deeper, more dynamic information sharing along the lines that we've talked about in cyber in the cyber domain. So, it's really interesting. You should talk about it in those terms, because I think it's important.

Christie, I'm going to come back to you in just a second to talk through how you with the SEC, and maybe even the government reviewing collaboration, which is a key word we've been using in this forum, collaboration with the regulated sectors? Obviously, you've got to police them. You've got to monitor. You

have to enforce. But what -- where collaboration is? But before that, Dante, I want to come back to you on this question of the ecosystem.

Can you, from your vantage point, explain to everybody what the ecosystem looks like? We know what the bad actors look like for the most part, right? We know what the state actors look like. We know the Russians were behind NotPetya in 2017, WannaCry, the North Koreans same year. We know DarkSide was behind the Russian organized group behind the Colonial Pipeline. It's other groups like FiveHands and Revil. I mean, it sounds like Marvel villains.

(Laughter)

MR. ZARATE: Talking about superheroes, there's Marvel villains out there. But they're real world, you know, hackers and ransomware groups. Can you speak to the environment and lay out the scope? Because I want to get to this question of what does a more proactive public/private partnership or model look like?

MR. DISPARTE: Sure. And I suppose in being asked the question, I need the disclaimer that, that I

don't know who all the bad actors are.

(Laughter)

MR. DISPARTE: But I do know that we have increasingly good tools and sort of forensics and a number of approaches that are becoming normalized, and how to combat them. So, I think crypto as a means of payment for ransomware really took center stage with the WannaCry attack. And the WannaCry attack again, partly driven by e-mail being the payload and being the sort of delivery vector, and then partly driven by exploits discovered by the U.S. government, in unpatched software platforms and Microsoft, but nonetheless, it was payable in Bitcoin. And over the course of a weekend, the WannaCry attack went from zero to 150 countries and collapsed entire sectors, if you will, especially the health care sector in the U.K.

Now, the economics of it are about $70,000 worth of Bitcoin was retrieved, payable to anonymous wallets. But because we could track and trace in near real time, it became increasingly difficult to extract the funds and launder the money and get the money out.

The second order economic effects however, and

this is really important. The second order economic effects may have been between $2 and $4 billion, nothing to do with the attack itself, nothing to do with a ransomware attack for economic gain, everything to do with underlying cyber vulnerability, lack of redundancy, lack of systems, lack of backup, lack of patching, keyboard and the chair, basic cyber hygiene.

And so, all of that to say the bad actors are manifold. I've spent an enormous amount of time with Secretary Ridge, sort, of looking at cyber resilience. The actor has to be right once. You have to be right 100 percent of the time to avoid the risk. The other piece of the puzzle with the advent of the prospect of cyber terrorism, where there is zero economic motive, and the only goal is to sow havoc, or distrust and to use these same delivery methods, but they have no economic motive. Who cares if you don't or cannot pay in cryptocurrency or Bitcoin if the attack is politically motivated. That's where we have to address the underlying cyber vulnerability.

The last quick point I would make, maybe I completely ignored your question conveniently.

(Laughter)

MR. DISPARTE: The last quick point I would make, because I think this is the nexus of U.S. policy responses. It's exactly what our colleague from Anchorage just mentioned, right? That today, we asked Colonial Pipeline to answer for its cyber resilience. And -- but meanwhile, the real exposure is a systemic exposure, kind of like the failure of one bank erodes confidence in banking. But we don't ask all banks in America to become resilient on their own. We figured out over years since the Great Depression, how to federalize and neutralize certain responses. I think cyber warrants a similar posture. So, I have a white paper for the National Defense University on this concept of a cyber-FDIC, destigmatize threat reporting, neutralize economics and risk sharing, and start to create a posture in which is deep public private collaboration. Until we do that, the exposure is never going to go away. And every sector, the large and small, is at the mercy of this type of vector of attack.

MR. ZARATE: Dante, well said. Christie, I

want to turn to you on this question of both regulation and enforcement, plus collaboration, feeding off of what Dante just laid out.

We know DOJ and DHS have the ransomware task forces, The White House has elevated this issue to an issue of national security import. From your vantage point, how do you view that balance between needing to regulate in a traditional way but also needing to collaborate to protect the U.S. financial and investment market?

MS. LITTMAN: It's a great question. I think, you know, I don't think that they're mutually exclusive. I think, you know, when we recognize that the SEC that it's a company, a public company, or a registered broker/dealer, investment advisor, has experienced a cyber incident that they're the victim. So, you know, while we balance that against their obligations to investors to provide adequate disclosure, or in the case of a registered investment advisor, broker dealer, their obligations to have policies and procedures in place to protect customer information, we recognize they're victims. We

recognize that they're in the middle of, you know, a cybersecurity incident that they're trying to get their arms around. They're trying to understand the scope of it and stop it. So, we don't expect their disclosures to include, you know, technical information about the systems or the network or the devices that are breached. We don't want them to expose potential systems that may have vulnerabilities, things like that. We don't want them to -- we want them to remediate incident. We don't want them to provide a roadmap for other threat actors. And for our part, we are also looking for those threat actors, right, to the extent that that those threat actors are trading on information, relating, right, if they're committing insider trading relating to the attack, we're on the lookout for that. So, we're always looking for trading around these incidents as well for our part.

And I'll say, you know, touching on one of the points that Georgia raised about, you know, kind of the market structure aspect of digital assets, which are obviously often used to pay for these ransomware attacks. We also are looking to partner with private

industry there. Our chair has been very open recently about wanting these entities who are often currently operating outside of the regulatory regime, wanting them to come in and register with us. If you're operating in exchange for digital assets, or some other market intermediary where you're transacting in digital assets, you should come talk to us and see how you fit into our regulatory regime, so that you can be a trusted participant in the financial markets.

MR. ZARATE: Thank you, Christie. Georgia, let me come back to you on what you're seeing in the marketplace. Because you're touching different aspects of it, obviously, from the regulatory standpoint. But you're also seeing the private sector actors that are having to deal with the realities of being attacked and having ransomware attacks and having to potentially make payments. Can you speak a little bit to the audience about what you're seeing and what you're hearing in the marketplace? And frankly, how you're thinking about it from an institutional perspective?

MS. QUINN: Sure. So -- and Dante hinted at this a little bit earlier, but what we're seeing is a

like plethora, extreme growth in tools and forensic services, to be able to trace these assets. And so, where I would, you know, like, two or three years ago, it was, you know, pretty, pretty slim chance that you were going to be able to find these assets and know, you know, who maybe the ultimate beneficial owner of a wallet was, and now we have just an incredible capability to trace this.

And one really unique feature of digital assets, which kind of sets it apart from traditional banking are the forward and backward ability to track every single transaction that's ever taken place in the lifecycle of this asset. So, when you're, you know, doing transaction monitoring at a bank, like just a traditional bank, you have a very slim snapshot of what's taking place within that bank. You know where that extends assets to, and you know where that bank proceeds assets to, but you don't know the third and fourth and fifth step after that, versus with digital assets, you can see in a very transparent way where that asset has been since the moment it was minted or mined, to, you know, where it sits today. And having

that capability is extremely powerful. And we are, you know, just now developing the analytical tools to use it, you know, in a way that's very, very helpful to trace these nefarious acts.

One other thing I wanted to make sure we touched on, again, kind of broadening the scope of the discussion to the greater kind of national security topics is this, the advent of stablecoins. And this, you know, there have been a lot of discussions about this lately. And I know, Treasury and the President's working group are looking into this asset class very, very carefully. At Anchorage, we really believe that stablecoins have the opportunity to further our national interests and strengthen the security of both our financial system and just the general welfare of the United States, in that, because the majority of stablecoins are backed by the U.S. dollar, and to the extent we can continue to promote those types of stablecoins, it allows the U.S. to play a very dominant role in the global financial system. We mentioned earlier that, you know, with crypto, there are no borders. It doesn't stop. You need at least a federal

if not global, regulatory overlay. And to be able to utilize the U.S. dollar to be the global currency of choice would really allow the U.S. to continue its dominance in the financial sector. And to the extent we choose not to pursue a digital, you know, stablecoin or similar asset, we feel that it could, you know, lead to a lot of detrimental, you know, consequences for not just our financial system, but our national security as well.

MR. ZARATE: Georgia, I'm glad you raised that, because the question of America's ability to retain its predominance in the financial commercial system, its ability to define norms internationally, regulates the cornerstone of U.S. power, the ability to use sanctions, anti-money laundering rules, all the things we've done traditionally, not to mention innovation and all the rest for our economy.

So, I'm glad you raised it, because in many ways, the crypto domain represents the domain of competition internationally. And Dante, you've written about this, you've thought about it obviously at Circle. You've issued USDC, which is one of the

stablecoins that Georgia is referencing. And we're seeing globally a question and a competition, if you will, around central bank digital currencies, and China's talking about it. Russia's talking about it, the Feds thinking about it. So, how do you think about that global competition, Dante, and the role of stablecoins?

MR. DISPARTE: Yeah. Well -- and I'm grateful to Georgia as well for bringing that point up. Because right now, in the policies sort of apparatus of our financial system, there is a conversation and more than a conversation and experimentation taking place called Project Hamilton, on whether or not the United States should try to out China, China on building a digital dollar of its own. In the interim, there is this entire $100 billion or more of dollar reference digital currencies that are in existence of which the one I support, a project called USDC is about $30 billion of dollar reference digital currencies. That private sector is existing, it thrives, it's globally competitive.

And the big public policy questions I think we

need to answer are, do our financial needs take bank holidays? Do they stop? Look backwards at COVID-19 in the onset in a domestic setting, and think about the things we could not do as a country with the movement of money at population scale. $6.6 trillion of intervention later, the people who were the most vulnerable, all of our country was subjected to getting a physical check. We couldn't execute a domestic payment in real time, we couldn't do it in a free way, we couldn't do it in a peer-to-peer manner. To me, that's a domestic national security vulnerability. And then we can't do that at population scale around the world, but for the very technologies that we've been discussing here. And so, I think failure to continue innovating, failure to pull these innovations on side and increasingly build them, I think, to the points that we were making earlier inside the line of sight of U.S. regulators, U.S. values, U.S. principles, would be to miss out on what the future of money and payments looks like.

MR. ZARATE: Yeah, I think we have a very natural segue for the next forum, where we have to talk

about the national security implications, positive negative of the crypto economy writ-large, and you've already touched on a number of them.

Let me open it up. We only have a few minutes here. But I want to open it up to the audience for any questions for our three, deep subject matter experts. I'm happy to pretend and weigh in. And let's see if there any questions. If not, I'm happy to add, ask more questions on my own.

All right. Well, let me ask this. Georgia, you alluded to a desire to have a more proactive sort of engagement with regulators. In a maximalist sense, what does that look like? What would be your dream world for how we collaborate in the ransomware context and in the crypto economy?

MS. QUINN: Thank you for that. So, I think what would be ideal is a partnership where we would work hand in hand with law enforcement, and we would provide the technology and the infrastructure that allows for the custody and the payment of the asset, in addition to the tracking and tracing and utilize, you know, what law enforcement does best, which is, you

know, go get the bad guys, and be able to not be in violation of our Bank Secrecy Act duties. I think that there's a huge promise for this type of product. Again, not just from the, you know, the kind of demand that we've seen, but just the commonsense reality of it. I mean, we saw what happened with Colonial Pipeline. If we could do that each and every time one of these ransomware payments had to be made, it would probably prevent, you know, the utilization of cryptocurrencies as a payment for ransomware, not ransomware itself.

MR. ZARATE: It's great answer. Let me ask in the closing seconds here, a lightning round of both Christie and Dante. There's one thing you would wish for in dealing with the threat of ransomware and obviously, the growth of the crypto economy. What would you want to see happen, whether it's on the government side or the private sector side? Christie, what do you think?

MS. LITTMAN: I think specifically with respect to SEC registrants like investment advisors and broker dealers, what we want to see are policies and

procedures that are designed to protect customer information.

MR. ZARATE: Got it. Dante?

MR. DISPARTE: And for me, simply put, we need the digital fire brigade here. And we need them to be able to work together collaboratively, irrespective of the size of their firm, whether in the public or private sphere, we need the digital fire brigade here.

MR. ZARATE: Rob Walker with your indulgence, I'm going to take one question. One question, sir, please. With the mic. Thank you.

MR. WATERMAN: Hi. I'd like to ask the panel what -- now that the White House has decided that this is a national ransomware, is a national security threat, what capabilities of the intelligence community and the national defense establishment would they like to see brought to bear on this problem that aren't being brought to bear right now?

MR. ZARATE: Sir, it's a great question. Your name please, in affiliation.

MR. WATERMAN: Shaun Waterman. I'm a journalist with README.

MR. ZARATE: Perfect. Thank you, Shaun. Georgia, you first, Christie, then Dante. Quickly.

MS. QUINN: So, just so I understand the question. What does the White House Want to see? Or what do we want to see?

MR. ZARATE: What would you want to see in light of the White House's actions and calling this a national security priority? What would you want to see from the intelligence community and others?

MS. QUINN: I would like to see resources allocated to our particular asset class specifically, you know, to do private partnerships, as I mentioned, and also make sure that research education is done, you know, throughout all levels of government to actually understand the power of this asset. And, you know, really, I mean, it's such a perfect solution to this problem when you think about the ultimate transparency of blockchain. And so just the ability to have resources to continue to further develop these tools that we're using, and, you know, put these kind of sting nets into place.

MR. ZARATE: Christie, posing the question to

you. Anything you'd want to see from the IC or the national security establishment to support you and the work you do?

MS. LITTMAN: I think it's important that we continue the kind of public private collaboration that you have been talking about today, sharing information, sharing ideas, and really, you know, working together with some of the groups that the presidential working group has already spun off. Certainly, we at the SEC are committed to doing that.

MR. ZARATE: Great. Dante?

MR. DISPARTE: Quickly, I would just say two things. First, the Chinese have chosen to have a digital renminbi or the Yuan on the internet, and they're exporting it through the Belt and Road, and they could process $60 trillion or more a year in mobile and internet native form. We do not have an answer as a policy matter. And I think that's one item that should come from the White House.

The second is we need a privacy preserving way of having digital identity. And the use of money in all of its forms should be the -- should inherit the

presumption of privacy in a series of first principles. We don't currently enjoy that today. And I think that too, is a major vulnerability.

MR. ZARATE: The closing remarks from me would be that this -- the crypto economy is not going away. It's part of the system. Ransomware is not going away as a threat. And we need to view this as a domain of both competition, threat risk and opportunity and apply the kinds of resources we've done in the counterterrorism context, the cyber context, and the same way that we've done in the anti-money laundering sanctions. Well, we have to apply that to this context in this environment.

So, with that, join me in thanking the panelists.

(Applause)

MR. ZARATE: Dante, Christie, Georgia, thank you very much.

MR. CLARK: Juan, just a moment. Jeanne Meserve me to see you, you didn't meet your panel expectations.

(Laughter)

MR. CLARK: She doesn't understand crypto yet. Let's give it up for the best dressed man in national security, Dante. All right. Quick 10-minute break, folks. Please be back in your seats at five after. We're trying to get back onto schedule. Thanks.

* * * * *