Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

Wednesday, July 19
2:45 - 3:20 PM MST
Sanctions, Scams, and Schemes: Cross-Sector Collaboration to Combat Financial Crime
Aaron Karczmer, EVP, Chief Enterprise Services Officer, PayPal
Brian Nelson, Under Secretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury
Matt Olsen, Assistant Attorney General for National Security, U.S. Department of Justice
***Moderator*: Mary Louise Kelly, Co-Host, All Things Considered, NPR**

Mary Louise Kelly
Hello, everyone. Welcome to the third panel of the afternoon. If I'm not mistaken, I can say with confidence This is surely the most civilant panel of the security forum sanctions, scams and schemes. So welcome we have with us representatives of private sector here with Aaron from Pay Pal and Brian from Treasury. Matt joining us from the Justice Department we are going to get to money laundering, cybercrime, ransomware cryptocurrency how AI is changing the game or not. What gives you hope? What gives you nightmares? I want to start with a quick level set and lay on me your best 6 second swing at this each of you how does your work look different than had we been on this stage five years ago, like cast your mind back 2018 What feels the same what feels different? And I want to start there because I want to give people a taste of just how quickly things are moving. We'll start the end Aaron.

Aaron Karczmer
Hello everyone. Great to be here. Such a fantastic event. And it's a great icebreaker question. So thank you. As I reflect back, you know, five years, it's been a really interesting five years geopolitically COVID and it's changed a lot of things certainly for us in the way we do business. And I would say the theme would be accelerating trends, right. So from a commercial perspective, accelerated the trend of offline transactions to online or business correspondingly grew from 200 million plus customers to know well over 400 million plus customers. 6 billion transactions to over 20 billion transactions a year. That's a huge playing field for us. 20 billion 20 billion transactions average value $60 for each. So very interesting playing field for us commercially, but also in my role to protect to protect those customers and those transactions and the other accelerating trends we saw on the bad actor side, right, they are getting more sophisticated and attacking more at scale than ever. And I think COVID and COVID Relief is a great example of the last five years right COVID relief as we've all read, scams are estimated between 200 and $300 billion dollars not for PayPal just overall. But we certainly did our part to combat that. And we always have a dual role. And we want to stop the bad actors. We also want to enable our good customers. So if you think about unemployment, fraud relief, we had to quickly pivot to deal with that scale And sophistication, while simultaneously ensure that our customers who needed those relief benefits could get them. That's a really good paradigm the last five years. Okay.

Mary Louise Kelly
All right. A few from Treasury. Say what looks different than a few years ago.

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

Brian Nelson
Okay. Aaron, well describe what we're seeing on our side. You see, sort of the explosion of in terms of the new payment rails and opportunities to move value across the globe has exploded exponentially over the last five years. So

Brian Nelson
as basic as we all Venmo know exactly. That;s not a dig at you.

Aaron Karczmer
We own Venmo.

Brian Nelson
And then, and then that obviously creates just opportunity for cyber enabled crime. So we've seen an explosion as well. Ransomware extortion, particularly hitting the United States, but globally, we've seen the proliferation of these dark darknet markets where you know, drugs and your ID, your credential and private information is sold again to facilitate ongoing illicit financing criminal activity. So I think we recognize that this actor could be anywhere in the world. So, but one thing that I've seen our government do and continue to do well to really push work international solutions to these challenges recognizing the United States when we're getting into a new focus

Matt Olsen
Yeah, thanks. Thanks, Mary Louise, and great to be here. I mean, if I could expand that question, actually, to 10 years ago, I sat on the stage and I was the director of the National Counterterrorism Center. We talked about the rise of ISIS and we talked about attacks in the United States and now at the Department of Justice. We still care about terrorism, international and increasingly domestic terrorism but but really now the focus as much as anything is on the intersection between national security and financial crime and corporate enforcement. And by you know, I think about export enforcement keeping sensitive technologies in the United States from getting to our adversaries for sanctions enforcement. Russia invades Ukraine, we go after all the guards and pursue sanctions, evasion, cybercrime that you've talked about. So the our work has really shifted significantly, really just in light. of the threats we face and what we're looking at in terms of nation state adversaries. And I would say the other thing which fit the theme of this panel is how much that work isn't just the federal government terrorism, largely the federal government, when we talk about financial crime, in our security partnerships with the private sector because they are on the front lines of this fight.

Mary Louise Kelly
Okay. I want to make this specific because it's so big and abstract and an art to get your head around and you mentioned Brian darknet markets. Let's do a little bit of a case study because there were big headlines some of us may have seen last year, a Justice Department investigation led to the shutdown of the hydra market, which per your press release that you'll put out was the world's largest and longest

running dark net market. helped me understand what what does that mean, what wasn't what was happening on this platform?

Brian Nelson
I'm happy to Yeah, so in addition to partnering with justice, we designated hydrq at the time and you know, the things that you see on these darknet markets is one a lot of drug trafficking. So we do worry a lot about drug trafficking organization, selling fentanyl and other opioids, synthetic opioids on these markets really fueling what we have seen in terms of the growth in fentanyl related deaths and here in the United States. So that's a critical national security concern another thing that you see is the selling of these credentials, so that you know your social security number can be sold on these markets and they've been exfiltrated through security, a cybersecurity breach company or your house your home information so that they can create a synthetic version of you apply for your credit, etc, or otherwise, try to profit off of your information

Mary Louise Kelly
Who's selling, where are these people?

Brian Nelson
So sometimes they can be anywhere in the world unfortunately, but a lot of these darknet markets are being relied upon by cyber criminals operating in Russia. So that's a common jurisdiction that we see. But truly, these actors are acting everywhere in the world.

Matt Olsen
Yeah, I think it's also illustrates the partnership between the Justice Department where I and the Treasury Department with Brian is Brian and his team has the sanctions authorities. We have the enforcement authorities behind those sanctions. So with hydro we work closely together. We actually charged the individual who's responsible for running the document website. And I think it really is, to your point, Brian, it really does highlight how sort of the digital asset ecosystem can fuel a whole range of illicit activities. Again, whether it's drug trafficking and fentanyl, or, you know, from an national security perspective ransomware and the movement of funds that support authoritarian regimes. So there's a there's a range of types of activity, but the thing that you think about is Hydra and other darknet marketplaces like it are the fuel for this illicit activity, and we have to bring all our tools to bear across the government to go after it.

Mary Louise Kelly
and just trying to understand the international aspect of it because I was fascinated. This was a DOJ takedown but the servers and the cryptocurrency wallet seized, Why does that matter if you're dealing with a currency that's all online? Anyway, talk about that partnership and why it matters, what country you're in.

Brian Nelson

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

No, I mean, I think where the servers are matters a lot to be able to actually take down the website. So for us, it's always a conversation is like what is the disruptive effect we got we have tools within our the USG but then it does have a foreign partner also have a tool that's going to lead to some disruptive effect. The thing that we don't want to do is take an action that's not actually going to disrupt the criminal activity that we're we're seeing so in this case, working with the Germans was critical to actually getting the service taken down because they have the legal authority to do that.

Mary Louise Kelly
And you said you charge the main guy. What's now that they know how to do this, are you already seeing copycats? How do you prevent that? Well, I

Matt Olsen
I mean, yeah, I mean, I think this is a challenge to be honest, that we all face which is these these nefarious actors take advantage of the boundary of this you know, nature of dark market ransomware you know, cybercrime generally and we are living in a world sort of physical world with in terms of law enforcement with you know, we want to arrest the person who's responsible and put them in a courtroom in the United States. And, you know, we put them in prison in the United States that that's not always possible. So we look for other ways to carry out disruptions. And that sometimes can be as basic as just announcing and highlighting the kinds of things we're seeing through our indictments through our charging documents, so that we can put them on notice but also put, you know other actors and achieve some degree of general deterrence because we say, Hey, we're watching you and we're gonna win. We're gonna go after you.

Brian Nelson
I think that is definitely true that these you take one down and oftentimes you see them proliferate in another jurisdiction. But Hydra actually was so big. I think. We have not seen that There's been a darknet market of scale, that size anywhere near that size, developing the time that we we took it down.

Mary Louise Kelly
Let's go to AI, a thread running through so many of the conversations this year. Speaking of we were this was on the radar five years ago, but nothing like it is now to make it specific, Aaron I know that people y'all talked about how AI is enabling fraud as a business model. E

Aaron Karczmer
Sure. Well, one, you know, AI is a big topic, and it's been around for a while and money law that you have on machine learning. You have aI now you have generative AI, right, and that's like the next big step. That's what we're all talking about it because it's a game changer, right. And so, and it's a game changer for everyone. And one of the ways to think about it is because it enables the machine to now make the next decision. It lowers the barrier of entry for everyone on different topics. So whether you're starting a business to do Photoshop, you know, to make pictures Well, now you don't need the training that you might have, right but the bad guy side, right, which is another trend we've seen over the years

and you will do an amazing job taking them down but you see the bad guys not just creating and using their capabilities to defraud people, but rather they build the tools and they sell them. Right. And so now with generative AI, they can do that at scale, right. And they can actually create API driven products with product releases. And you can have fairly low level people on the bad actor side participating in very sophisticated attacks.

Mary Louise Kelly
Give us an example.

Aaron Karczmer
So we can set up so think about I know another hot topic is ransomware. So ransomware you know, the bad actors go after people's emails and trying to convince them well, with generative AI, those are going to look more real than ever, and you'll be able to operate that faster and with more frequency than ever and by the way, you don't need to know how to do it. You can buy it from someone else on the dark web, and then deploy it against the company. And so it's going to be much harder to detect the sort of real from the fake and so it will no doubt, if not deterred by us and others turned into much worse cases.

Mary Louise Kelly
How is Paypal how's the private sector generally thinking about using it in good ways? How's it healthy?

Aaron Karczmer
So AI has been part of our DNA for a long time. Right. So one of the lifeblood for our company is we want to enable all these transactions all over the world. We also want to make sure we're not taken advantage of and don't lose too much money. And so we've been investing on the cutting edge of these technologies, including these types of, you know, margin language models for many years, actually. And so that continues to be on the bleeding edge for us. So we'll continue to invest there to make sure that we can protect our platform and our customers. Because if we don't we know that the bad guys will continue to expand their capabilities. And so we always say in fraud. If you're not staying one step ahead. You're behind. There's no There's no maintain.

Mary Louise Kelly
To what extent are you able to police it? What's the view from law enforcement on this? I know you'll just set up a new thing With the disruptive technology strike. What is that?

Matt Olsen
Yeah. So I mean, when we think about artificial intelligence from the Department of Justice standpoint, from the FCC, and when we think about how we protect our development of these sensitive technologies, these are used it in game changing technologies that PayPal, other companies, the government are developing, and that really allows us to stay a step ahead of our adversaries, whether it's in the military context, intelligence, or just general technology. And so we have laws that protect the

sensitive technologies AI, first among them from being transferred illegally to our adversaries. And so we set up this year, a new strike force called the disruptive technology Strike Force focusing on AI and other technologies with the Commerce Department which has authorities in these areas to enforce export controls and make it so that together as a as a team, we are preventing these sorts of sensitive technologies from illegally being moved outside of the United States, because these are the technologies that have literally have the capacity to alter the balance of power between the United States and our adversaries.

Mary Louise Kelly
How well is it working?

Matt Olsen
Right now it's working pretty well. I mean, we just started but I will say, we announced about five cases a couple months ago. One of them was a case involving a software engineer who worked at Apple who took stole apples, some of Apple's AI technology and proprietary technology and went to work immediately for a company in China. And he's been charged now buying and for allegedly engaging in stealing Apple's proprietary technology. So we are working again very closely with the private sector who are at the forefront of developing these technologies to make sure we're in a position to protect them.

Mary Louise Kelly
Want to jump in on this one?

Brian Nelson
We're focused One of our roles at Treasury is we work to protect critical infrastructure, obviously focused on financial institutions. So recognizing that technology is going to create opportunity, obviously, as Matt noted book on the national security side, as well as opportunity for adversaries and bad actors out there. We're focused on a couple of things like resilience, not just in the context of AI but you know, coming quantum and other disruptive technologies, as Matt noted, and then and then working with, with private sector partners, frankly, to understand how bad actors are using these tools and what they're seeing.

Mary Louise Kelly
Staying with new technology and things we might not have been talking about on this stage 5, 10 years ago, cryptocurrency I have a bunch of big general questions, but I guess I've been struck by recent headlines of major players in that field going belly up. How does that impact your work from a purely just trying to stop Financial Crimes point of view setting aside convenience profitability everything else? Is this a good development?

Brian Nelson

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

I don't know if it's good or bad. I think we come from a couple of perspectives with the basis is we want to support responsible innovation. And the way that we see that happening is for cryptocurrencies firms, virtual assets, service providers, to really build in meaningful money laundering and terrorist financing and compliance in the service in the app or on their blockchain. So that's, that's critical from our perspective, number one, and then, you know, number two, I think what we have see we've done some illicit finance risk assessments both in the context of digital assets and specifically decentralized finance. And in both cases, what you see is there are a lot of these virtual assets service providers that are subject to AML CFT compliance and sanctions, screen rules and they are not following those and that is, frankly, the biggest source of risks because it is no surprise that the bad actors know that if these companies aren't doing that screen or have an AML CFT compliance, that they can run whatever form of illicit finance they want through that service. So getting compliance is sort of the first step for us and then obviously avoiding the scenario where you have these companies jumping from jurisdiction to jurisdiction to try to avoid medieval compliance. So working globally through the Financial Action Task Force, which sets AML CFT compliance across the world is a key part of the efforts that we're trying to test.

Aaron Karczmer
So share respectives, you know, also, obviously for Responsible innovation, and, you know, we believe in embracing new technology and understanding it and being the responsible player in it. And so for cryptocurrency, one, there's many, many facets to it, but at the end of the day, whether it's whatever the new technology is, there's always concern but it's still moving money from point A to point B. And what do you know, point A, what do you know, the point being what do you know in between, and cryptocurrency is very interesting because as you just shared, sometimes in point A in the beginning, you don't know that much. Right? But you know where it ends up, but here's the really interesting part. Cryptocurrency runs on the blockchain, which is technology that actually has an immutable ledger, meaning once something happens there, it's there forever. And that's very powerful evidence for law enforcement for us who like to help law enforcement. So there's a lot of tools out there that actually are enabling the government and private sector to crack really extensive global syndicates who are using cryptocurrency so I think there was a way that the bad actors felt like this was really going to protect them in a way that they're seeing now that those funds are actually being grabbed. Right, sometimes they're being grabbed. And so I think some demystification is helpful and I think there are responsible ways to participate in what will no doubt be part of commerce.

Matt Olsen
Yeah, just a brief comment on that because I totally agree with you guys comments and he'll be and adjustments are closely with companies responsible companies with good compliance programs and who are committed to corporate governance and governance and working with with the with the government. It is the case that crypto by its nature by its decentralized, pseudo anonymous, direct intermediaries, it does that is why those features features of crypto that help it become the fuel for ransomware. And from an aesthetic perspective, the biggest concern I think, crypto for us is how North Korea uses crypto patient by stealing it and they steal it to support their weapons program. So you can

see immediately why that's such a big concern for us. They, I think probably reports are that they stolen 3 billion with a B dollars worth of crypto since 2017. And we've taken steps to get working with responsible corporate actors and our partners in the Treasury Department and elsewhere to basically seize and freeze some of this crypto. So it can never be actually used, some of that just sits on the blockchain not available to the DPRK for example, to build missiles.

Mary Louise Kelly
Are there specific challenges though and going after activity happening are linked to North Korea?

Matt Olsen
When the anything linked to North Korea, it's gonna be hard, right? But it is a it is a newer problem for us and we're thinking about how we can be innovative in really being able to trace to your exact point here and like there are we have some capacity to trace these guns so that we can take steps to prevent it from ultimately making its way into the supporting the weapons program, the DPRK

Mary Louise Kelly
speaking of specific countries, one of you mentioned, a lot of the bad guys are trying to go after are in Russia are linked to Russia. Have you seen any impacts in the war in Ukraine? Have you seen any impact from Russia decoupling from the global economy in many ways getting kicked out of Swift etc. has that impacted activity, illicit financial activity you're saying that's Russia linked?

Brian Nelson
It has. So at the beginning of the conflict, there was a lot of concern that Russia would try to use these other financial rails to evade our sanctions. And I don't think we've seen that sort of at scale yet. That you know, the capacity to move billions and billions of dollars and then cash that out meaningful Lee we're still not seeing that and obviously an economy of the size of Russia, not able to do that. What we have seen though, is the development and and interest in developing new payment relationships, but our financial relationships with countries in Russia's near abroad and one of the things that me and my colleagues have been going around talking to partner countries and countries that are again sort of in Russia is near abroad that they would use to try and ship the things that they need on the battlefield about sort of the consequences of materially evading us and partner and ally sanctions. And that our priority in this context is really making sure one that we are restricting the revenue that Russia has in order to continue to prosecute this war, but to an equally and more critically restrict the Russia's ability to continue to get the material parts and stuff that they need on the battlefield to continue to prosecute this war.

Mary Louise Kelly
When you talk about Russia's near abroad. You're talking about the caucuses, wherever

Brian Nelson
Vaucus is UAE, Turkey, jurisdictions like that.

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

Mary Louise Kelly
Sounds it's really hard. And it's really, really hard.

Brian Nelson
That's why it was a lot of partner engagement. I think one of the benefits of Matt noted, you know, why do we designate these wall as why do we designate companies people is because financial institutions around the globe that want to have continue to have access to the US financial system have to follow those designations. So that's a really wide net. So it creates a lot of opportunity to disrupt a lot of the illicit financial flows.

Mary Louise Kelly
Speaking amongst friends has the last year and a half with the invasion of Ukraine and everything that's happened with Russia since made it harder that people you can't reach anymore because of sanctions.

Matt Olsen
I wouldn't say it's made it harder I mean, it you know, I think some really important successes and coming together both as a as a as a federal government but also with international partners to go after all of our ducks and others who are supporting the Kremlin to make the point that we are going to go after their assets and not only their assets, but those that facilitate them. So we started a task force come to capture Task Force and sees over $500 million arrested or indicted over 30 individuals. So I think this is making a difference. Look, there are always gonna be people who are beyond our reach, but they can travel. They can't live the lives they're used. To lighting living, they don't have their yachts anymore. So look, I think I think it works and I think it works over time. As Brian said, Moscow's ability to to continue the war.

Mary Louise Kelly
I'm gonna open it up to questions from all of you in one minute. Hold that thought I see you. We'll come to you in one minute. I want to quickly before we're all incredibly depressed. Do one more quick we'll go down the road this time this way. What gives you hope? That's like a really good development. Yes. Super excited to talk about.

Matt Olsen
look, I mean, I talked about the intersection between national security and financial crimes and one statistic that really jumps out at me is that in the last year or so, literally two thirds of the corporate resolutions that we brought in in the Justice Department have involved national security, two thirds, almost $2 billion in financial penalties over the past year involving corporate wrongdoers, so my hope is that we are making changes within the next year division. We are I can say today we now as of this week, have a new chief counsel for corporate enforcement. We wouldn't have seen that five years ago, who has been have a team dedicated to bringing your corporate enforcement in line and the way we've done in other contexts like like, like fraud and corruption. And now in the context of sanctions and

export enforcement and cyber, we're taking that same sort of national security approach to that problem. So I do think the partnerships that we're going to develop through that type of program with companies like PayPal and others, along with the increased focus within the Justice Department decided to go reason to be hopeful that we're going to make a dent when it comes to overall corporate

Brian Nelson
You know, honestly, I think for for me, as you all can imagine, the bulk of our interview over the last 18 months is really largely been focused on all we can do to support Ukraine in this war, and the thing that gives me a lot of hope is just how resilient united the coalition partner and allies have been and developing together tools in order to go after the Russian elite and the oligarchs and proxies to Putin to really constrain Russia's ability to continue to prosecute this war and that resiliency has, you know, manifested in a ways that we've all seen including the adding up new members of NATO, so that gives me a lot of hope for.

Aaron Karczmer
I would say, cross, you know, cross collaboration across private sector, public sector and also the nonprofit sector. So that gives me continue to, I've seen throughout my career, that the results we get together is always better than we can do individually. And I see that cresting, right even Brian, you know, we had teams together in Texas last week, talking about fentanyl, right, like 300 people every day in the US dying, right? And so, through the collaboration, we promote we get trained on like how do you make fentanyl what chemicals are the precursors? What amounts and that enables us to then monitor and provide information back to actually disrupt these bad actors. And so the fact that that's working, so Well, absolutely gives me hope.

Mary Louise Kelly
And that's just like tagging purchases. Correct? Yeah. Well, it's suspicious that you wouldn't have known

Brian Nelson
what what are they seeing that suspicious? What indicators? Are we learning through our partnerships with DOJ, FBI, DHS, and then how can we better identify sort of the financial tracing that we support going after these actors?

Mary Louise Kelly
Okay, we're gonna try to get into questions. Yes, ma'am. In the back if you would tell us who you are adequate. Question.

Audience question
Hi, Joanie Lee back, former vice president American bison and Cultural Foundation longtime local part of the Aspen mountain seems to be have sold to a possible Russian oligarch who possibly seemingly gave his assets to his mother as Swiss citizenship. And I'm wondering if the DOJ or Treasury is aware of this problem, and if we can get our land back.

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

Matt Olsen
So we'll talk okay you and I. Look, I mean, stepping back then, we did. We are very concerned about the way that some of these assets can be hidden through very sophisticated means. And again, working with the Treasury Department, other partners, including the intelligence community, one of the one of the stories behind cup to capture, task force is the work that we did from intelligence to understand how these oligarchs were moving and hiding their money. So it does your question does highlight some real challenges in this area,.

Mary Louise Kelly
So quick point upfront, if we can, we'll get to these two.

Brian Nelson
Can I just offer one comment on that just stuff because it goes directly to what we're doing in Treasury which is developing a beneficial ownership reporting requirement that will come into place early next year and then to Matt's point looking at real estate transaction and investment advisors because these are very opaque ways of transferring value within our financial system.

Audience question
My name is Claire Finkelstein, I'm a faculty member at University of Pennsylvania Law School and I run a center called Center for Ethics and the rule of law, which is a national security and Ethics Center. One of the areas that I've worked extensively on that I thought might come up in this discussion is foreign agent Registration Act. One of the tools in DOJ toolbox, maybe not the strongest tool, but I'm just wondering especially question for you, Matt. There have been some revisions they served on the ABA committee that recommended certain revisions to FARA, and how do you regard FARA among the tools in your toolbox for addressing some of the issues here?

Matt Olsen
Yeah, I appreciate the question, Claire, and I know the important work that you do at this Baker Center, University of Pennsylvania so Farah, the foreign agent Registration Act is really a transparency law. That requires individuals who are acting as agents of other governments to to register so that we basically know the United States if, if a foreign government is seeking basically covertly to influence our politics, and we've used this rather sparingly over the years, but the point you're making is a really important one is that we're looking to really clarify and strengthen How would us give the team that enforces this pitch loss and additional civil authorities some additional ways to be so they can gather more information, but the real goal is to address what we call foreign malign influence. So you think about China and Russia and Iran in particular, and their abilities to influence our politics or you know, our, our policies. And so we need to have laws in place that help place a bright light and make sure that those efforts are transparent.

Mary Louise Kelly

Note that this is an automated transcription and may contain inaccuracies. Please refer to the original YouTube recording as well

All right under the wire, we have 60 seconds, and I've seen this gentleman stand right here.

Audience question
Hi, I'm Bruce Mcgever, chairman emeritus of Berkshire Capital Advisors. These panels get on the same subject get better every year. So congratulations to you , guys. However, I'm wondering why we talk about this every year but we don't have as a country the cyber police. Why don't we do something about this?

Mary Louise Kelly
Cyber sick repeat Cyber

Matt Olsen
Police. Police complete Oh

Brian Nelson
so we you know now as of two years ago, we now this director of cyber security I don't know what his or former title is operating out of the White House which I think is important coordinating feature. And then obviously DHS is doing a lot of important work in the cyberspace as well, but it is a whole of government effort.

Matt Olsen
We're much better off than we were a few years ago in terms of how the government organized between the White House department Homeland Security FBI, DHS treasury. I'll give you a just a quick example. We worked at relevant to this topic. We work very hard to claw back some of the ransom that was paid in the Colonial Pipeline ransomware attack in 2021. We actually were able to use our intelligence authority section seven up to a FISA to get that information back. And that's an example I think of, you know, we talked about cyber police, using all of our authorities intelligence and law enforcement to be better at protecting our companies in particular from cyber attacks.

Mary Louise Kelly
it was a very skillful and quick plug for 702. Thank you for the question. And I think you've teed us up for opening the conversation next year. So