Consumer Finance Monitor (Season 9, Episode 23): White House Executive Order on Scams and Fraud Takes Center Stage

Speakers: Alan Kaplinsky, Kate Griffin and Nick Bourke

Alan Kaplinsky:

Welcome to the award-winning Consumer Finance Monitor Podcast, where we explore important new developments in the world of consumer financial services and what they mean for your business, your customers, and the industry. This is a weekly show brought to you by the Consumer Financial Services Group at the Ballard Spahr law firm. And I'm your host, Alan Kaplinsky, the former Practice Group Leader for 25 years, and now Senior Counsel of the Consumer Financial Services Group at Ballard Spahr. And I'm pleased to be moderating today's program.

For those of you who want even more information, don't forget about our blog, which also goes by the same name as our podcast show, namely Consumer Finance Monitor. We've hosted our blog since 2011 when the CFPB became operational, so there is a lot of relevant industry content there, including content about the subject that we're going to be talking about today, which I will summarize for you in just a minute.

We also regularly host webinars on subjects of interest to those in the industry, so to subscribe to our blog or to get on the list for our webinars, please visit us at ballardspahr.com. And if you like our podcast show, please let us know about it. You can leave us a review, Apple Podcasts, YouTube, Spotify, or whatever major platform you use to access your podcasts. Also, please let us know if you have any ideas for other topics that we should consider covering or speakers that we should consider as guests on our show. As long as the topic deals with the consumer finance world, it's fair game for our show.

So, I'm going to tell you a little bit about the topic, and then I'm going to introduce our guests today. First of all, want to welcome back to our show to guests that have been on several prior episodes of our show. And I'm referring to Nick Bourke and Kate Griffin of the Aspen Institute's Financial Security Program. We did a program on February 26th of this year in which we discussed in detail Aspen Institute's landmark report entitled United We Stand: A National Strategy to Prevent Scams. It's a comprehensive, first of its kind effort developed by a national task force of more than 300 experts across government, industry, and civil society. As we discussed in that February 26th episode, the report makes a compelling case that scams and fraud have become a whole of society problem requiring a coordinated cross-sector response.

So today, we're going to build on that conversation by focusing on the White House's recently issued, that is on March 6th of this year, Executive Order 14390, which is called Combating Cyber Crime, Fraud, and Predatory Schemes Against American Citizens. We also blogged about that Executive Order on our Consumer Finance Monitor blog on March 24th, so I would commend that to your reading.

What's particularly interesting, and the reason I wanted to bring Nick and Kate back again is that this Executive Order appears to pick up on several of the core themes and recommendations that were made in the Aspen report. For example, the Executive Order emphasizes a coordinated federal strategy, enhanced public-private information sharing, and a more aggressive effort to disrupt transnational criminal organizations operating scam centers abroad. In many ways, the Executive Order can be seen as an early federal response to the very gap that the Aspen report identified, the absence until now of a truly coordinated national strategy to combat scams. So today, we're going to explore how closely the Executive Order aligns with the Aspen recommendations, where the Executive Order may fall short, and what it means for financial institutions, technology companies, and policymakers going forward.

But before I do anything, let me properly introduce our two guests. First, I want to introduce Kate Griffin. Kate is the Director of Inclusive Financial System at the Aspen Institute Financial Security Program. She led Aspen's National Task Force on Fraud and Scam Prevention in 2024 and 2025, and recently launched the Scam Prevention Initiative, which is bringing together corporate leaders to collaborate among themselves with law enforcement and others on efforts to combat fraud against consumers and small businesses. So Kate, a very warm welcome to you.

Kate Griffin:

Thanks so much. Happy to be here again.

Alan Kaplinsky:

Great to have you, Kate. And Nick, Nick Bourke is a senior policy advisor with Aspen's Financial Security Program. He has more than 20 years of experience in public policy, market research, and law, including as a former co-founder and leader of the consumer finance and housing programs at the Pew Charitable Trust. So Nick, also a very more and welcome to you.

Nick Bourke:

Thank you, Alan. Happy to be here.

Alan Kaplinsky:

Okay. So let's get into it, and I've organized my questioning today under a few categories. And the first category I call it framing the Executive Order versus the Aspen report. In our last episode that we did on February 26th, we discussed how the Aspen report called for a coordinated national strategy to combat scams. At a high level, do you view the Executive Order as delivering on that recommendation? And the follow-up, of course, is why or why not?

Kate Griffin:

Thanks, Alan. And I appreciate your kind words about the report, and about how you see it show up here in this Executive Order, that action. We view this Executive Order as a really exciting moment. If you think about it as a race against scams, the Executive Order has lined up all the stakeholders at the start line and pulled the trigger on the starting gun. We're off to the races now. And in fact, if you look at the report, the highest priority thing that we had in there was for the government to really treat this as a national priority and direct a coordinated effort. It's really the start of doing that, but what's really important is what comes next. We now have the opportunity to do all of the other things in the report or many of the other things in the report as a result of having this directive. And we're keenly looking to see what happens next in terms of the delivery of a federal action plan later this year.

Alan Kaplinsky:

Okay. The Aspen report emphasizes its scams are, and I think it's referred to in the report as a whole of ecosystem problem requiring coordination across government, financial institutions, telecom and technology platforms. Does the Executive Order adequately reflect that cross-sector approach?

Nick Bourke:

Well, not completely, but it definitely makes a strong gesture in that direction. It's an Executive Order, so it's very government-centric. But as Kate said, it's lining up a lot of different actors that are across different jurisdictions. I think one important thing to note is that the Executive Order talks about using the National Coordination Center, the NCC. That's something this White House created as a way of coordinating different agencies across the government to fight crime. So using the NCC for scams is a great step.

In Aspen's work, one thing that we've been really focused on and we've seen a need for is bringing together a lot of different parts of the private sector underneath that. I think what you're seeing in the Executive Order is the federal government starting to organize its own cross-sector ways of communicating and coordinating with one another, and the next key step will be getting the sector regulators and the industries that those sector regulators regulate aligned and coordinating and exchanging information and coordinating on action as well.

Alan Kaplinsky:

Okay. Well, let's talk about coordination and governance. One of the Aspen reports, key ideas was the creation of a centralized front door or national anti-scam center to coordinate reporting and response. Do you see the Executive Order's proposed inter-agency coordination, particularly the NCC operational sell as a step in that direction, or is something still missing?

Kate Griffin:

Like with many things in this Executive Order, maybe. It depends on what happens next. It's an interesting opportunity in that it really directs a number of different agencies to say, "Here's what we think we need to do to get better at this and how to utilize the National Coordination Center." It depends on how those agencies decide to use that opportunity. Will they come and say, "Gosh, the conflicting reporting requirements that we have between all of these different law enforcement agencies and the portals should be fixed and we can use this opportunity to do that"? If they are able to have that conversation and make meaningful steps towards that, then it's a great opportunity. But it really depends on what happens next and how the leadership within those agencies take advantage of the opportunity they have to contribute to this federal action plan.

Alan Kaplinsky:

Okay. The report also highlighted fragmentation in federal reporting systems and the need for better coordination. I should say the Aspen report highlighted it. Does the Executive Order meaningfully address that issue?

Nick Bourke:

Anecdotally, we're hearing that since the Executive Order came out, different parts of different federal agencies are getting assignments to interact. The Executive Order requires, it's probably worth mentioning, it requires a number of different departments, War, State, Attorney General, Treasury to all contribute to making a plan through the NCC, through senior White House advisors, all the way up to the president. And it requires this plan to be done by July of this year. So they are sprinting. And anecdotally, we've heard that a lot of different parts of a lot of different agencies are tasked with helping.

We don't know what they're talking about. I would therefore assume that the CEO gives them a lot of great opportunities to talk about the specific things that are relevant. To your question, the EEO gives a lot of different people in government the chance to talk about the things that we talked about in our task force, which would be modernizing FBI's IC3 database, modernizing the FTC's Sentinel database, modernizing FinCEN's SARs database, and not just their databases, but the way that those databases are able to ingest and onboard information.

So I have to presume that when the White House says they want more coordination among federal agencies and better information that they're talking about these things, they really should be. And when we talk about a national front door, that's the next step down the road where we've got the plumbing in order at the federal level, now we're making it a much more simple, singular task for the public and for companies to go to a place where they can serve up relevant scam related information for the government.

Alan Kaplinsky:

Let's turn now to the area that's in the Aspen report dealing with public and private information sharing. A central theme of the Aspen report is the need for robust, real-time information sharing across the private sector, including banks, telecom companies, and platforms. The Executive Order calls for greater use of private sector cyber intelligence. Is that enough?

Kate Griffin:

Probably not. It's a really important step in terms of creating pathways for the private sector to be using that intelligence more effectively with law enforcement, and hopefully a result of that will be greater investment in the resources that law enforcement needs to ingest and take advantage of that data. We hope that that's a result of the contributions to the federal action plan and what comes next from it. It does less, because it's an Executive Order, as Nick pointed out, it's really dealing with what is within the powers of the executive branch. And so it does less to catalyze private sector to private sector

information sharing, and likely that'll be more a job that Congress needs to do, but it's an exciting step forward in terms of making sure that we're getting more information and better back and forth with law enforcement.

Alan Kaplinsky:

I take it, Kate, you don't think that this could be done by, I guess a less formal type of law like a regulation by various agencies and you think it is going to actually require a statute.

Nick Bourke:

I'll jump in on that. I mean, I think it's a both and thing here, Alan. The thing that I think we should all really celebrate in the Executive Order is that it's a very clear public policy and leadership statement from the White House saying scams are a national problem and fixing the scam problem is a national priority. That is what the Executive Order is really good for.

Underneath that, everybody in federal agencies should be asking themselves, what do they need to be doing to empower the industries that are relevant here? We're talking about banking, we're talking about telcos, we're talking about social media and digital platforms. What should those federal agencies be doing to empower those companies to get better at fighting scams and giving law enforcement leads to go after scam criminals? They obviously can't do that on their own though. They're going to need some regulations.

They're going to need to be guidance just to say, "Here's the best way to share information among yourselves without triggering privacy concerns, without triggering concerns about getting sued, without triggering antitrust concerns." And obviously, some of that's going to have to be more formal, so we're going to have to talk about at some point some legislation.

Alan Kaplinsky:

Yeah, sure. I guess it's going to have to be at a minimum some exemption from the antitrust laws for information sharing of this kind, I would think.

Nick Bourke:

I would think so. I mean, at least a very narrow specific carve out or codified pathway to do some certain things, yes.

Alan Kaplinsky:

Yeah, okay. The report also raised the importance of safe harbors to encourage companies to share data without fear or liability. Is there anything in the Executive Order about that or is that a little bit too granular at this point?

Nick Bourke:

They don't exactly call for any safe harbors, but I would say again, that by calling it out as a national priority and directing the government to federal agencies to get their houses in order, I think the Executive Order is tantamount to, like Kate says, the starting gun. Here's the start where federal agencies need to be thinking about the safe harbors they need to be providing to their industries.

Alan Kaplinsky:

Okay. All right. Let's turn to another part of the Aspen report, law enforcement and disruption of criminal networks. The Aspen report stresses the importance of disrupting the scam business model, not just prosecuting individual actors. Does the Executive Order's focus on transnational criminal organizations and scam centers reflect that shift?

Kate Griffin:

This is another really exciting element of what we see in the Executive Order is really calling out who these criminals are and organizing the government against that threat at that level is one of the most important recommendations that came out of our report and from what the task force was asking for. If you can shift the mental model of who this criminal is to one that

recognizes the sophistication of the criminal networks and that it is in fact highly lucrative business, it's a really important framework to be using when you think about what are all of the ways that we prevent and disrupt these kinds of crimes from happening, and shifting that mental model away from thinking about how do we stop an individual victimization to how do we stop this crime happening across all of society, I think really forces each of these agencies to think about their work in a really critical way.

Alan Kaplinsky:

Right. And to think of it not just as a United States issue, right? I mean, there's a large component of this criminal network is outside the US. Some of it is even supported by some countries, and so there's going to be a need to, I'm sure, to think about how do you deal with this thing on an international basis. The Executive Order contemplates a more assertive international posture, including sanctions and diplomatic pressure. And of course, maybe I've already answered the question, but let me ask you what you think, how important is that global dimension to the success of any national anti-scam strategy?

Kate Griffin:

As you pointed out, these are transnational criminal organizations. They are largely operating overseas and some of them have connections to very sophisticated crime rings and sometimes the governments of the countries where they're operating. We have to deploy all the means that we have necessary. We've already sanctioned individuals that we believe that are closely aligned with these criminal enterprises. We've seen the beginning of some kinds of diplomatic pressure and some cooperation with other governments like in the United Kingdom to do this. The Executive Order really calls in the State Department, the Department of War, the Treasury Department, all of the powers that each of those agencies have are going to be critical in this fight. I think it's a really important measure to recognize that those powers are just as important as all the things that we're talking about in terms of law enforcement and information sharing. They're an equally important part of this equation.

Alan Kaplinsky:

Let me ask this question. Are there similar initiatives that are going on in other countries and as any attempt being made right now to coordinate with the United States, with other countries that are already doing things, and some of them may be further ahead than we are?

Nick Bourke:

Yes. The UN recently held a meeting, and maybe Kate will want to comment on that because she was more involved in it, but Interpol, the UN, these types of multilateral agencies have been focusing on the scam problem. Individual countries have been intentionally collaborating with one another, Australia, the UK, Singapore. Even China has been noted as recently getting more involved in identifying and going after certain scam compounds in Southeast Asia. It's definitely recognized as an international crime problem. I don't know. Kate, did you want to add anything about the UN process?

Kate Griffin:

Well, so Nick's referring to the UN Global Fraud Summit, which happened about a month ago in Vienna, and it was a really important display of a number of different countries sending delegations at the ministerial level to showcase what they are doing in their own fights against scams and how they are wanting to cooperate together. The Executive Order was issued, I don't know, a week or two before the UN Global Fraud Summit, and a number of government officials from the US government attended that event. And I think it's an exciting step forward in terms of really seeing global convergence on the scale and scope of the problem, and the interconnected nature of how we have to cooperate and collaborate with one another and with the private sector, which was there in attending this event in spades. So it was, I think in some respects, really exciting to see that this many different global actors were coming together in alignment on the severity of the problem and the necessity of collaborating together to fight it.

Nick Bourke:

I'll add something too, the White House created a scam center strike force towards the end of last year that specifically directs various parts of the US law enforcement intelligence and foreign relations departments to collaborate together specifically to identify the biggest transnational scam operations that are operating in Southeast Asia. A lot of times, these criminal networks are maintaining compounds where they have sometimes forced labor conditions, people working in these scam compounds whose job it is to call and text and do all the things that we see on the other end of that as spam email and fraudulent phone calls. The strike force that the White House set up is intended to focus resources on going after those compounds, but here's something really cool and interesting about that and how it relates to the Executive Order.

Even the utmost law enforcement and intelligence operations in the United States, when they're focusing on scams, they're recognizing that it's not simply a law enforcement issue. It's not just about going after the bad guys where they are working. Because it's an issue that's affecting all of our platforms, all of our banking platforms, our digital social media platforms or telecoms, they're recognizing that they have to do more to protect those systems from the bad communications getting onto them in the first place. And so it's this really interesting melding of law enforcement ideas with ideas about information sharing from corporations and empowering corporations to get better at intervening on their own platforms when they see evidence that their customers are at risk of encountering scams.

Alan Kaplinsky:

Okay. Thank you, Nick. So let's turn to the next segment that I would like to talk about is victim protection and restoration. The Aspen report emphasizes improving the victim experience, including reporting and recovery. How significant is the Executive Order's proposed victim restoration program in that context?

Nick Bourke:

I'd say it's significant and it's symbolically important. We can talk about numbers like the FTC's estimate that American households are losing now close to $200 billion a year to scam activity. It's really difficult to imagine the magnitude of the loss on the other end of that. If you're a household that's making $50,000 or $100,000 a year and you lose $15,000, $20,000 to a scammer, or you lose your entire $200,000 retirement fund is devastating. It's devastating if you're making $300,000, $500,000 a year, but it is really devastating if you're making a more modest income. So the White House gives an important nod to that, and it lines up with Aspen's strategy because there has to be a consideration of helping victims to recover. And it's not just about money, it's also about just simply knowing where to turn to report the problem. It's about knowing where to turn to get resources and to help correct, protect their accounts from getting accessed again, so it's a really important symbolic move.

I think it's good that the EO, in this sense, focuses on more seizure and forfeiture of scam assets because the scam criminals are using digital assets of all kinds to take money from people, and if law enforcement has better powers to seize that money and force its forfeiture so that it goes back to the victims via this victim fund that the EO talks about, that could actually put a lot of money back into people's hands.

Alan Kaplinsky:

Let me clarify something with you, Nick. Fiat currency you're saying is not used or it's not generally used, so are you saying that in order for these criminals to perpetrate their scams, they've got to get their victims to convert fiat currency into cryptocurrency? Is that what happened?

Nick Bourke:

That's just one use case. I actually don't know the data offhand. Maybe Kate does. I think most of the scams are still executed via fiat currency, the victim sending fiat currency typically electronically from their bank account to somewhere else, but where sometimes it's that the customer, the victim is convinced to say, take out cash from the bank and then go to a crypto ATM where the cash is instantaneously turned into cryptocurrency, which disappears to the scammer's account. I think where cryptocurrency probably comes in more is that it's a really fast and convenient way for the criminals, once they get the fiat currency, to convert it into a form that they can then maybe bounce around to a couple different wallets inside of the country,

and then they bounce it out to a cryptocurrency wallet outside of the country. And even though through blockchain, it's all technically traceable, it becomes operationally impossible to trace that once it's gone.

Kate Griffin:

I just want to jump in here though too, in terms of the way that the Executive Order frames this as a victim restoration program. Last year, there was a historic asset seizure of $15 billion of funds related to these kinds of fraud and scam schemes. And today, there's not necessarily a very easy way for victims to make a claim against that asset seizure and say, "Well, these funds are mine. How do I get them returned to me?"

There are other differing incentives within that system too, in terms of the ways that law enforcement, whether it's an asset seizure from cyber crime or any other kind of crime, is also using that funding in order to help them go after even more bad guys. There are other uses of that fund that are also important to society, and so really naming that we need to create a fund that allows for an easier restoration to victims to make them whole again is a pretty exciting and novel part of this equation, and we're certainly very interested to see how that bears out.

Alan Kaplinsky:

Yeah. Your Aspen report noted that many victims don't even report scams due to confusion or stigma. They're embarrassed to say to anybody that they've been bilked. What more needs to be done beyond what's in the Executive Order to address that problem?

Kate Griffin:

I think there are multiple things we can look at here. First of all, from a communications perspective, the more that we can talk about these kinds of scams as something that, A, is happening to many, many people, there's nothing to be ashamed about, and that the perpetrators of these crimes are quite sophisticated transnational organizations. You didn't fall victim to something silly or trivial, you were targeted for a very specific kind of crime. So the messaging that we use about this kind of crime really matters. In fact, the way that the Executive Order talked about it was really powerful and the call-in of transnational criminal organizations, so that's one.

And then second, the fact that it does talk about a victim restoration program is exciting. Sometimes people don't report, yes, there's confusion about where to report, and that confusion also is because oftentimes there's very little result to reporting. The ability to have law enforcement respond and help you actually get your money back is minimal. There are some important cases where there are heroic law enforcement officers at a local, state and federal level doing that, but it's certainly not the story that you hear from many victims. The more that we can build a response for victims when they do report that is meaningful, the more that I think we can reduce the incidences of under-reporting.

Alan Kaplinsky:

Right. I guess there needs to be a lot of emphasis placed on education. I mean, there's not a lot that I see just in general. I don't think I've ever seen a public service announcement on TV or anything. Maybe others have seen it, but I've never seen it. I know a lot of the crime is perpetrated against elderly people, they tend to be more vulnerable. And elderly people do congregate in certain places. Some of them might be in homes where they're being cared for, and my guess is they can even be vulnerable there. The Aspen report remind me, do you go into a lot of detail on the need to educate in advance of the crime actually occurring so that when somebody gets targeted, a light bulb immediately goes off in that person's head saying, "Sounds like I might be being scammed here."

Nick Bourke:

Alan, one thing I want to say clearly is you can't educate your way out of a global criminal enterprise phenomenon. Education's not going to solve the fact that transnational criminal organizations are systematically preying on households through very technologically sophisticated means. That said, we definitely talked about awareness, consumer awareness. And one of the lessons that came out of our task force was it is really important to get coordinated on the messaging that we give

to people as people who care about the scams issue. It's good if people have a very clear message, so protect yourself is a good message.

It's like we all know if we're walking down the street at night in a rough neighborhood, we don't walk around with a bunch of cash in our hand. You've got to have good safety hygiene. That said, you don't want to scare people too much because we want them to have trust in the systems that they're using. It's important, the better we get at giving people a single place to go to report and a single place to find resources, it's important that we get better at having a very clear message. Have you been scammed? Go to scams.gov or stopscams.gov. That's really important. Training for people in sensitive positions like bank tellers or people working in old senior homes, good to have some very clear training about how to spot problems. But that's like hygiene. It's good hygiene for protecting against this stuff, but really, it doesn't replace systematic efforts to take down the scams business model.

Alan Kaplinsky:

Yeah, got it. Let's talk, as we wind up this podcast, about the future and what I'm going to call any gaps in the Executive Order of what comes next. So if either one of you or maybe both of you had to identify one or two major recommendations from the Aspen report that are not fully reflected in the Executive Order, what would they be?

Kate Griffin:

I'll start, and then I know Nick will want to chime in there. I think the first thing we've identified already, which is the Executive Order, because it really directs the agencies within its jurisdiction, does what it can in terms of what that branch of government needs to do in order to play its role in a whole of society response. We still need the private sector and Congress to take actions as well. And so the extent to which we are excited by, for example, the private sector's recent release of a set of industry accords at the UN Global Fraud Summit that outlined certain steps that the companies that signed onto those industry accords would want to take as an example of an exciting kind of corollary process. We need to see those kinds of initiatives as well from the private sector and as well as from Congress.

Alan Kaplinsky:

What about you, Nick? Anything that you'd like to add to what Kate said?

Nick Bourke:

I'll drill in a little bit on modernizing law enforcement's capabilities. I think the more that the Executive Order and federal agencies place emphasis on having law enforcement agencies focus on getting better at detecting and disrupting scam activity and going after scam criminals, the more we focus on that, the more we're going to realize that law enforcement doesn't have sufficient tools. There are some very clear things that need to happen. It's talked about in Aspen's report about a national strategy.

We talked about it a lot in our task force so a few of those things are... So there are these databases that law enforcement relies on constantly. FBI's IC3 database, FTC Sentinel. FBI's database is where a lot of crime reporting goes to. Sentinel takes crime reports, but also consumer complaints. FinCEN's SARs database is where banks and financial institutions send suspicious activity reports when they suspect that something is going wrong. These are all very important databases because when a federal prosecutor wants to find concentrations of illegal activity, they go to these databases and mine them, and then they form prosecutions.

All of those databases were designed before the scam era. They were designed for a slower, more individual transaction level kind of analysis. None of them are really suitable to the kind of real-time aggregation of information and high volume analysis of trends and just the superfast analysis that has to happen. So whether we're talking about the federal agencies just getting better at modernizing those tools to the extent they're able to, or probably Congress getting involved and directing and funding more of that modernization, that's super critical to success going forward.

Alan Kaplinsky:

Yeah. To what extent, Nick, is AI important in this effort to attack the criminals that are scamming?

Nick Bourke:

It's a tool that I think most people would agree law enforcement could get a lot of benefit out of. Obviously, there have to be safeguards on AI when you're using sensitive information. I think we can presume that law enforcement is pretty experienced with handling sensitive information appropriately. The problem is that those databases where the information comes from are, sometimes they're on 20 or even 30-year-old operating systems. AI is only as good as the data that it has available to it, so it's another both and thing. We need better data, and then we can start layering better analytical tools on top of it.

Alan Kaplinsky:

Sure. And when you talk about providing tools to law enforcement, are you including local law enforcement, state and local law enforcement, as well as the FBI and federal agencies?

Nick Bourke:

I think that the emphasis and the focus is and should be on federal agencies, particularly because they are the ones who are always tasked with identifying the foreign bad actors. I think where local law enforcement comes in more, it's not that they don't need information, they do. But I think where local law enforcement issues probably come in more is having better, more standardized training about how to spot scam activity and what to do when they find it. Most scam activity now happens digitally and local law enforcement may never see it or touch it, but sometimes you do have people who are money mules who are going around to people's houses, collecting cash because of some scam that's going on.

Or sometimes you have crypto ATM rings where they're encouraging people to go to banks and take out cash and go to the crypto ATM and put the cash in. Local law enforcement needs to know how to spot that stuff, but more importantly, they need a really clear standardized message of what to do and who to report it to at the federal agencies when they see it.

Alan Kaplinsky:

Okay. My final question, look into your crystal ball and share with our audience what success would look like a year from now if both the Executive Order and the Aspen strategy are effectively implemented. Let's say a year from now. I'm not going to go too far out.

Kate Griffin:

Alan, we've already always framed the goal of this work as that the work should undermine the scams business model. Nick mentioned the $200 billion a year figure, right? That's a Fortune 50 company. It's huge, and it exists because all of these parts of the ecosystem have made it so that it is an incredibly lucrative business. It's cheap to implement with high revenue, high profit margins, and low possibility that you're going to get caught, or that the consequences are going to be very severe. If we are able to disrupt that business model a year from now, we'll see a lot more in terms of criminal prosecutions.

We'll see that when take down occurs, that there are the speed at which the criminals just gin up the next set of infrastructure activity that that has started to slow down. Essentially, our measure of the efficacy of our scam prevention work in undermining that business model will start to see incremental progress within a year. That's how we'll know whether it's been successful because that's what it's going to take to eradicate this.

Alan Kaplinsky:

Do you want to add anything, Nick?

Nick Bourke:

Kate's spot on. I mean, a year from now, we're not going to be able to declare victory against scams, but if we can say there's a clear federal strategy, if federal agency mechanisms like the NCC are activated in helping to coordinate federal agency activity, if the White House is talking about scam prevention and encouraging business leaders to invest resources in it, if we're actually seeing some big prosecutions, all those things that Kate mentioned spot on, we need to undermine the scam business model by making it harder, less lucrative and riskier for scammers to operate.

Alan Kaplinsky:

Okay. Well, let me wrap things up first of all by thanking both Nick and Kate for joining us again and further continued leadership on this critically important issue. As we've discussed today, the White House Executive Order represents an important step toward what the Aspen Institute's United We Stand Report called for, a coordinated national response to the growing epidemic of scams and frauds. The report made clear that the US has lacked a unified strategy and that no single sector can solve this problem alone. The Executive Order begins to fill that gap, particularly in its emphasis on inter-agency coordination, public private collaboration, and targeting transnational criminal organizations.

But as Nick and Kate have highlighted, fully realizing the vision of the Aspen report will likely require additional steps, especially legislative action, clear rules for information sharing, and continued cross-sector collaboration. Ultimately, I think the key takeaway from both the Aspen report and today's discussion is that combating scams is not just a law enforcement issue, and of course, law enforcement is integral part of what needs to be strengthened here, but it's a systemic challenge that requires close alignment across government, industry, and civil society, and we'll be continuing to follow these developments.

And by all means, Nick and Kate, please let me know next time something significant happens because we'll want to have you back on the show to talk about it. So again, my thanks to both of you, and I also want to thank our listeners for downloading the podcast show today and listening to this very important development. Thank you all, and I hope you enjoy the rest of your day.