ICANN83 | PF – ccNSO: DASC Online Scams and Financial Crime
Wednesday, June 11, 2025 – 13:45 to 15:00 CEST

CLAUDIA RUIZ: Hello and welcome to ccNSO DASC Online Scams and Financial Crime Session. My name is Claudia Ruiz and I, along with my colleagues, Joke and Julie, are the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior and the ICANN Community Anti-Harassment Policy. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted. Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak, if speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation. Thank you. And with this, I will now hand the floor over to Nick Wenban-Smith.

NICK WENBAN-SMITH: Thank you. Thank you, Claudia. First of all, I should introduce myself. For those who don't know me, I'm Nick Wenban-Smith from NOMINET, the .UK ccTLD, and I'm, for the time being, chair of the

ccNSO's DNS Abuse Standing Committee. Today's session, I think, is going to be a very interesting one, and it has been prepared with a bit of build-up through the previous meetings and a bit of focus on what it is that we wanted to have a deeper dive into, what are the priorities for the ccTLDs from all over the world. So I'm very pleased to be able to chair this panel of proper experts and really interesting content. And it's also supposed to be interactive, so very much welcome questions. I will try and keep an eye on the Zoom room, but staff will, I'm sure, keep me on the straight and narrow.

We are on quite a tight timeline, so I just will introduce very briefly my fellow panelists, starting in the order on the screen. Gabe, if you could just introduce yourself and just say a little bit.

GABRIEL ANDREWS Thanks. Hi, my name is Gabriel. I am co-chair of the Public Safety Working Group here at ICANN, and my day job is working for the FBI back in the U.S.

NICK WENBAN-SMITH Thanks, Gabe. Keith?

KEITH DRAZEK Good afternoon, everyone. My name is Keith Drazek. I work for Verisign, and I am responsible within the company for our DNS abuse mitigation program, in addition to managing our ICANN

multi-stakeholder policy team. So very happy to be here, happy to be back in the ccNSO room. Some of you may remember me back when I worked in a different company and a different life working in support of .US. I was one of you. Glad to be back. Thank you.

NICK WENBAN-SMITH Thanks, Keith. Mon, can you hear us, and can you put yourself off mute and just introduce yourself, please?

MON PEREZ Yeah, I can hear you. So my name is Mon. I am a technical manager at SGNIC, so I'm in charge mostly of running the operations for the .SG domain name registry. Also, I have been tasked back then to develop an abuse management system, so pretty much I also handle the domain abuse part. Thank you.

NICK WENBAN-SMITH Brilliant. Thanks very much. And over to you, Bruce, just a quick introduction.

BRUCE TONKIN My name is Bruce Tonkin from the .AU Country Code.

NICK WENBAN-SMITH Thanks very much, and thanks, Mon, especially for staying up. It's quite an antisocial hour in Singapore, so we really appreciate you joining online. As you can see from the slide, most of the

infographic photos of the panelists are pre-COVID, apart from Mon. So really appreciate it.

Okay, so just by way of a quick introduction and overview, this session kicks off essentially an exploration of the theme of online scams and financial fraud, and in particular the intersection with the abuse of domain names for perpetrating these sorts of crimes and the technical abuses and the societal impact. So this is more looking at the scale of the issue and then some presentations about approaches and challenges which remain. If we can move to the next slide.

So just a quick overview of the DASC, the DNS Abuse Standing Committee, and a reminder that we're not here to set policy for ccTLDs. That is done at a national level, but we are here to socialize important issues and to promote understanding and awareness. We want to have an open and constructive dialogue. But of course, at the end of the day, we are fundamentally interested in actually pushing down the amount of abuse of our ccTLD registries and to help everybody achieve that objective. So next slide, please.

So just as a sort of scene setting, in 2002 and 2024, we did a global survey of the ccTLDs. And this is an interesting legal word here, bifurcation. In terms of the ICANN policies, the gTLDs are very firmly in the remit of ICANN policy and the technical definition of DNS abuse. But what came through in these surveys is that many ccTLDs do not have this, as some would regard, a sort of semantic or artificial distinction between certain types of abuse and certain

other types of abuse. Most of us consider abuse to be abuse. And it came through that criminal content, for example, fraud, is a major issue. And actually, it is actionable and considered something that the registry would intervene on in certain situations. I wanted to highlight back to our Kigali meeting, where we heard particularly from the Africans and the Nigerian registry regulators in particular about the plague of cryptocurrency scams. Just absolute out-and-out fraud targeting vulnerable consumers and citizens in that country. In the UK, where I'm from, fraud is 40% of all crime, which is a huge amount. It's the biggest form of crime. And 80% of payment fraud originates from either social media or from fake websites. So this is an area which falls squarely into the remit of many ccTLD registries. And there's a high degree of overlap in terms of the technical definition of DNS abuse, which includes phishing. It's the major element of DNS abuse in the world. And obviously, use of phishing emails is an entry point to perpetrator financial crime. Our last meeting in Seattle, we settled on this topic. So I was just going to move on to the panel discussions now. Having said that, I'll just follow with the next slide, which is definition. Scams are fraudulent invitation, request, notification, or offer designed to obtain personal information or money or otherwise test financial benefit by deception. Frequently, but not always, a maliciously registered domain is part of that. Just next slide. So this session here is sort of an introductory session. We plan to do further work in the subsequent ICANN meetings. And you can see that we're going to broaden this out into a broader cross-community stakeholder conversation. There's a quick Mentimeter here at the

beginning of the session. So if we can move forward. So I'll give everybody a little chance. There's two Mentimeter polls. So I'm trying to give everybody a chance to capture it. It's one of the things I think we do very well in the ccNSO is using these interactive polls. Helps people for him. which is the majority of the ccNSO and it allows people to do that fine. So let's go on to the question if everybody is ready. Next slide. Okay, so the question is an easy question. To what extent is your registry prepared to well prepared to detect domain name abuse linked to financial crime? Give people a chance to ... Okay, this is not a precise scientific survey. It's just a sort of temperature of the room, flavor of the scale of the problem and understanding. So with that, I would like to hand over to Gabe to give his presentation. Gabe, the floor is yours.

GABRIEL ANDREWS All right. Can I see this next slide? Perfect. Thank you. So in Seattle, I was speaking with Nick and I had mentioned that the FBI's annual Internet crime report had just missed being published before Seattle and that it would be published soon thereafter. And he mentioned to me that it might be interesting to talk about it with you all. So I wanted to seize the opportunity and I thank you for the chance. This data comes from our Internet crime complaint center portal. And what that means is that anytime a victim comes to us and wants to tell us that they've been victimized, we route them through a single portal that really helps us to justify the investigative resources that we put at it to loop those cases together and the victims together. But it gives the added benefit of

giving us some pretty good statistics that we can then publish on an annual basis. Next slide.

I want to acknowledge that I am just a cop from a single country, but nonetheless, when we run these numbers, we see that we actually do receive complaints from more than 200 countries around the world, at least in 2024 we did. So, you know, Nick, the UK was responsible for more than 100,000, just as an example. This is reflective of the fact that cybercrime is global, right? So I do think that even though I'm talking about stats from the U.S., this is pretty representative of what my counterparts all across the world are seeing too. Next slide.

So what we do is we count how many complaints we receive, and then we also try to sum up how much loss is associated with each category of complaint and crime that we're hearing about. And I've highlighted a few on here. I hope you can read it okay. But on the left, when you go by complaint count, you can see that phishing is responsible by far for more complaints than anything else that we hear about. And that makes sense. We know that phishing happens all the time. And as, Nick, I think you just said earlier, it very much is the initial intrusion vector or the initial way that a lot of the other crime is perpetuated downstream. And then when you look to the right and try to total up, okay, where's the loss occurring? The very top category there is investment fraud, otherwise referred to as cryptocurrency investment fraud. And so my ears perked up when you talked about hearing from Nigeria about this and it being a plague. It is a plague. This is responsible for more than $6.5 billion

of loss in the U.S. in just last year in 2024 alone. It's also responsible for victim suicides when they lose their life savings. We'll dive into that a little bit. But I also wanted to spend a little bit of time on business email compromise, which is just a subcategory of phishing, and then talk a little bit about ransomware. Because even though it's way down there at only 12 million of loss, it's actually really a lot worse than that. I know it's not fraud, but it's just it was worth a moment. So let's go ahead and go into the next slide. And we'll talk about business email compromise.

This is your stereotypical phishing where a bad guy impersonates someone who's like the CEO, the power to initiate a wire transfer. And this is a real BEC email from when I worked this violation back in 2015 or so. We got permission from the victim to use this for educational purposes. If you were to notice the, I don't remember if this is another slide or not, maybe you could play with me and we'll just back up if it's not. But click one time just to see if there's a highlight. All right, I'm standing by. Yeah, there we go. So you can see that the actual subject here was impersonating the company Fly Jet Edge. They did a homograph lookalike domain name registration. And as an investigator, one of the first things I wanted to do is just say, okay, what's publicly available about that domain name? So you do a WHOIS lookup. And at the time, I might have seen the record very much like this. And one of the reasons I look at this is I want to know where can I send my legal process? Are they in my country? Are they in some other country? Where are we going

to have to go investigatively with this? Go ahead, next. Standing by for next. There we go. Awesome.

The act of submitting legal process, it takes a while. So let's say two or three weeks down the road, I've got the subpoena. I've sent it off. I get the results back. One of the things I might ask for is what are all the other domain names that this bad guy has registered? In addition to just this one that's targeting this victim that's reached out to me. And I might see that there could be a dozen or two dozen other domain names that they've registered that all using my super smart investigator brain, I can figure out are just like a slight misspelling of something that's probably real. And now my job is like in the midst of trying to do this investigation, I also really want to let those potential victims know that they're actively being targeted by the bad guy, right? And so one of the things I might do is I might not take the time to do additional two or three week legal process to each and every one of the registrars associated with those additional victim domains. But if I can find some good telephone numbers from WHOIS about those potential victims, I might be able to really prevent further harm. All right, click through.

Very similarly with ransomware, I was speaking with my sister agency, CISA, which is responsible for critical infrastructure protection in the U.S. And let's go ahead and jump to the next slide here too. And I just wanted to highlight that this is an entirely different category of crime. It's not fraud related, but what they have to do in their mission is very similar to what I just described. They are also very much in the position of trying to prevent harm.

And in their situation, you might have cybersecurity researchers that are watching known ransomware servers. And based off of their historical observation, they know that when a new victim is first seen pinging out to that ransomware infrastructure, then within the next 24 or 48 or 72 hours, they might have ransomware deployed on the victim network. And soon thereafter, it'll be activated and they're going to have a no good day. So the researchers will call that out to us. They'll reach out to CISA, to FBI, and we worked it together for a while. And they'll say, hey, this brand new victim IP is observed reaching out to that known bad guy. And then CISA has the ticking clock in how quickly can they convert that internet identifier to a conversation. And so they've also very much relied upon the availability of records, public records, to swiftly convert those internet identifiers to real world contact information. And it's a very important thing to be able to do. I think they saved more than eight and a half billion dollars of potential ransomware payments just last year alone over more than 2400 victim notifications. All right, next.

I'm trying to move swiftly through this here, knowing that we're on a clock ourselves. The cryptocurrency investment fraud. All right, we alluded to this before. It sounds like you've already heard about it from Nigeria. In the states, again, it is by far the most damaging loss category that we're seeing at more than six and a half billion dollars. The next highest was the [inaudible] at less than half that. Let's click through. I think everyone in this room is very likely to have been targeted by one of these at the start. It always starts with

just a WhatsApp message or signal or whatever your chat platform of choice is. And it always is innocuous to start someone that's trying to engage in a conversation. And there's some pretense. Maybe they're pretending that they were your vet or your doctor or someone else that it was a friend. And it's just a honest mistake that they're texting you instead of someone else. They will spend a lot of time trying to convert that into a conversation, convert that conversation into trust. And at some point later, drop into the conversation the fact that they just made so much money on such and such cryptocurrency investment platform. If you buy into that, you might be invested yourself very soon thereafter. If you buy into further conversations, you might think you're making a lot of money and put more and more of your life savings into this, as has happened. Go ahead and click to the next.

When they do this, they will run fake cryptocurrency exchange platforms themselves. They can be updated with real-time live data. So it looks tremendously real and authentic to the victims. When I talk to the case agents that investigate this, and we'll click through the next slide here, they tell me that the bad guys, Standing by for the next. They tell me that the bad guys will register hundreds of domains maliciously at a time in order to promote those fake cryptocurrency exchanges. So I just wanted to highlight this fact, that if you are maybe observing that there are bulk registrations being conducted through your ccTLD, that even if these domains themselves are not ccTLDs, they can and will use ccTLDs as part of this. The sheer volume of this allows them to

promote these exchanges. Even as one domain's taken down, they just shift to the next the next to the next.

A particularly challenging part of this is that when the investigators are looking at this, many times the registrars that are being used are not located locally to the law enforcement and there are some challenges that arise because of that and we'll go ahead. And click through to the next slide now. When we use publicly available information like on the left of this little diagram I made like Google or WHOIS resources, we can do these checks in minutes, right? Seconds or minutes. We do as cops have the authorities to send out compulsory legal process subpoenas or court orders, but that moves the timeline into more like days, weeks, maybe even month for a search warrant. When it crosses international boundaries, now we're reliant upon the only tool available to us, which is mutual legal assistance treaty requests. And from experience, those take me six to twelve months on average when I've done them in the past. It is not very conducive to swift-moving investigations. And so, the key point I make is that when we're able to voluntarily accept things like WHOIS data from ccTLD operators, even if we're not in the same country, it can really make our jobs a lot swifter in trying to find out more about the bad guys. So let's click to what I think is my very last slide. There we are.

So, a quick recap of just the points that I was going through here. WHOIS data is very helpful to cops around the world when we're trying to figure out where to route our legal process or court orders, and so on and so forth. If you do use resellers yourself, please list

them. I really don't want to have us sending legal process to the wrong entity just because we thought it was a registrar, but really it's something underneath the registrar. Public safety agencies absolutely want to be able to use WHOIS to prevent harm to victims. Cryptocurrency investment fraud is really no-good, bad, horrible stuff, and it involves registrations in bulk to promote fake exchanges. And lastly, voluntary responses to foreign LA—foreign law enforcement. If it's from a country that you respect and you think you can trust, voluntary disclosure can really help us, and even though I know it's always a choice and it's always user discretion. All right. So, I thank you all for your attention. I hope this is of interest and I'm very grateful even for the opportunity to talk. Nick, back to you.

NICK WENBAN-SMITH

Thanks very much, Gabe. Are there any immediate questions? I think the only thing I was going to say is that obviously a lot of the examples seem to be gTLDs, but it does affect ccTLDs. And from my perspective, although I may not, with all due respect, recognize the authority of the United States, if I receive something from the FBI and it's essentially pointing out a fraud, I'm not going to put it in the bin. There are other policies internal for each ccTLD. If you're given good cause to do further investigation, then there are processes for most ccTLDs which won't require the MLAT processes, because if we can see, for example, that it's manifestly fake registration data, there are much more expedited processes that most responsible registries would voluntarily follow. And I

hope we can talk a bit more about that. But let's move on to Keith on my left.

KEITH DRAZEK

Thank you very much, Nick. Hi, everybody. Keith Drazek with Verisign. I am here today to give an introduction to a new initiative called the Internet Infrastructure Forum. And I will get to the details in a moment. I'd like to provide a little bit of context and background as to why this is something that we are supporting along with a few others. In 2022, the gTLD registries and registrars recognized that we needed to take a step forward and to take the initiative to deal with the topic of DNS abuse as it was being discussed in the ICANN space. I think you all know the gTLD registries and registrars have contracts with ICANN. There had been 10 years' worth of discussion around the topic of DNS abuse. And we recognized that something needed to be done.

So we voluntarily engaged with ICANN, essentially offering and asking to take on new contractually enforceable obligations to deal with DNS abuse. And through that process, we defined DNS abuse with ICANN in our contracts as being technical abuse of phishing, farming, malware, botnet command and control distribution, and spam when spam is used as a delivery mechanism for those other four. And so having the term defined, the DNS abuse term defined in our contracts, we also recognized that there was going to be continued pressure on ICANN to get involved in content-related harms. And for those who may not be intimately familiar, ICANN's

bylaws prohibit it from getting involved in content moderation or anything like that. So we recognized that there was a need to develop another multi-stakeholder engagement point, a parallel track for discussion of online harms to include content, but to have that exist outside of the ICANN sphere, outside of the ICANN umbrella. So in parallel to the discussions around the contract negotiations, several gTLD registries and registrars got together and started talking about the need to develop what is now the Internet Infrastructure Forum. So Verisign, PIR, Identity Digital, Google, Amazon, and CloudFlare were essentially the six companies that came together recognizing that this was something worth pursuing, and that we wanted to engage the internet infrastructure operators engaged in content, hosts, CDNs, et cetera, to bring them to the table and to start talking about how we as internet infrastructure operators can work better together to deal with and to mitigate online harms more broadly than the defined term within the ICANN space.

And so this is an initiative that began really in earnest last year. We had our first face-to-face meeting that took place the first week of February in Amsterdam this year. We had 53 participants representing 38 organizations – slower, sorry – 38 organizations over a two-day meeting that was, I think, quite well received. We, the six companies that sort of came together to initiate this, worked very closely with the Internet and Jurisdiction Policy Network, and I want to acknowledge Bertrand de La Chapelle, who's here with us today. He is sort of the lead coordinator and facilitator for this effort

of the Internet Infrastructure Forum, and also working with ICO and their top DNS initiative and the Internet Infrastructure Coalition, I2C, based in North America. So that's essentially the core group of facilitators, those that are working to advance the goals of the IIF.

So coming out of the Amsterdam meeting, which was really important for us to sort of validate that this was a worthwhile endeavor, that there was consensus, especially among the web hosts and the CDNs and the cloud service providers who don't typically participate in the ICANN space unless they happen to have a registry or a registrar, but really to engage the content layer of the stack in these conversations. We really needed to validate that there was interest and a sort of a willingness to commit to engage in figuring out how we can better work together in a collaborative way, sharing information, identifying concrete topics to be able to help mitigate online harms within our respective roles, responsibilities, and technical capabilities, depending on the actual harm that we're trying to address. So coming out of the Amsterdam meeting, we identified four work tracks, one that's focused on legal policy and regulatory developments to include, at the time, DSA implementation and transparency requirements, NIS 2 transposition and know your customer issues, and GDPR and information sharing. This was a track that was identified to really help inform and support some of the other work that's a little bit more targeted in the second track is operational issues and automation, how do we develop systems that can facilitate the sharing of information, the routing of abuse reports with feedback

loops, so that the various actors in the stack will have the ability to communicate more effectively, more efficiently, to help us all address the harms more effectively. And then two of the substantive tracks, the first one is focused a bit on CSAM and NCII, non-consensual intimate imagery, but really the focus of that group is to talk about the role of trusted notifiers and trusted flaggers in the ecosystem of abuse mitigation. And the final track of the four is phishing plus, which is essentially noting that phishing, as Gabe mentioned, is one of the biggest sort of vectors of fraud, but it enables a lot of other types of fraud and abuse and online harms. And so that was the other category. So it's a really exciting initiative. We're at this stage of starting to want to expand the membership, but also to, or the participation, I should say, it's not a member organization, to expand the participation, but we also recognize we need to maintain balance between sort of the traditional DNS operators and to make sure that we've got the content layer and the hosts involved.

And I'm just going to wrap up here by saying that eventually, this is currently an industry-led initiative. It is really industry at this point. We're engaging with providers of services that engage in facilitating the mitigation of online harms. So we've got a good core at this stage. But the plan is to expand this work to ensure that we have some multi-stakeholder engagement, to make sure that we're engaging with other interest groups and other groups with expertise. And that's sort of the next step as we move forward on getting some of this work done, progressing this work, is to make

sure that we're having a multi-stakeholder engagement so we can ensure that what we're doing is well-informed. So I'll stop there. Thank you, Nick.

NICK WENBAN-SMITH: Thank you, Keith. And so part of the reason for including this subject in this presentation deck is because I think all of us are aware of the fact that just acting at the domain name level is only a sort of disruptive thing. You're not actually fundamentally addressing the content. So actually getting to the website host where the frauds or phishing or other online harm is being actually conducted is really the sort of the ultimate aim, because the disruptive activity you can take as a ccTLD operator doesn't prevent other domain names, whether it's gTLDs or ccTLDs, being spun up quite quickly and then pointing to the same thing. So I think that sort of perspective is a very interesting one to bear in mind as we go into these further discussions around these ultimately content related issues. So that's that. So let's move on now to Mon in Singapore for a little case study of how they've actually set up an initiative to fight against financial crime. Thanks, Mon. The floor is yours.

MON PEREZ: Thank you, Nick. Next slide, please. Okay, so to put it in context, we all know that financial crime is a major issue. So it causes financial loss and damages the public trust of .SG domain name. So I managed to get the report from one of the local search in

Singapore. So there were 8,000 phishing attempts in 2022. Luckily, none of them were from .SG. They were mostly from other ccTLDs. 80% of the phishing attempts were targeting bank and financial services, government and logistics. Next slide, please. So these are the abuses that SGNIC is concerned about. So just to put it in context, the first bucket is the abuses that ICANN is aware of or more concerned of. Phishing, spam, botnet and pharming. The second bucket are the abuses that SGNIC is concerned about. So those with asterisks are the things that SGNIC feels that we should do more. Later on, I will share what are the additional things that we have done. And then the last bucket is, these are not really abuses, but these are sort of indicators which our team does to detect early signs of potential abuses. Next slide, please.

Okay. So these are the preventive and detective measures that SGNIC has. So firstly, we have the verified ID at SG. So this ensures that domain name registration undergo verification using SINGPASS, which is Singapore's national digital identity. So it reduces identity theft. So basically, this is our KYC process. Secondly, we have registry lock, which is a free security feature to help that Azure registrant mitigate the risk of domain name hijacking or unauthorized modification. And then lastly, we have the abuse management system. This is an internal system that monitors malicious website pertaining to phishing or malware, and thereby, we alert the stakeholders to take necessary action. Next slide, please.

Okay, so I'm going to go deeper into the abuse management system. So basically, this was developed in-house. What it does is it detects and tracks domain name abuse, which I mentioned, mostly malware and phishing. And also, it does check for incorrect or suspicious registration information. It also checks for DNS water usage and bot registration. So the system basically flags for any of these potential domain name abuse. So when it's flagged, we are able to validate it, and then, if it's a confirmed case, we would then notify the stakeholders, such as the registrant, the registrar, and the hosting provider for the necessary action to take. Initially, SGNIC collaborated with a local search to provide expert opinion, because we were unaware of how to detect malware and phishing back then. But thereafter, there were commercial feeds that provide solution data. So due to that, SGNIC took over the role. So now, it is embedded into the system. Next slide, please.

So this is the other feature of the abuse management system. So basically, it detects for incorrect or suspicious registration. What it does is, given a company registration number, the system checks it against the company registration database, and then extracts the company name. Based on the company name, we then cross-check it with the company name that was registered to verify whether the registration is fictitious or not. Next slide, please. So here's another part of AMS. So basically, these are just CQ reports. So they provide us with insights on some of the common attacks and applications that are being targeted. So in a way, this just gives us a sense of what are the common abuse types, what are the common abuse

factors, or whether there is any spike in domain name abuses that we have detected. Next slide, please. So what has all these efforts brought to SGNIC? So firstly, we have zero reported incidents on domain name hijacking. Also, because we have a system now, so we are able to measure our resolution rate. So what we do is we ensure that we keep 80% of the cases being resolved per month. So that has been our target so far. Thirdly, we've been well-informed of ongoing or emerging threats. So just to highlight one notable incident, AMS was first built in 2010. So after it ran for a few years, there was an event in July 2012 where a popular web hosting platform was exploited. So this was quite noticeable in AMS because we were able to see around 100 .sg domain names being used for phishing. So because of AMS, we were able to find a common hosting provider. So what we did was we quickly called the hosting provider and asked their administrators to fix the issue and also to remove the phishing pages. So within hours the phishing pages were taken down. Next slide please. So another emerging threat that we also noticed with AMS, which was quite recent, is a compromised open source library in 2024. So we did some checks. The issue was due to a threat actor bought a domain name and also bought a GitHub account of a popular open source library. Because of this, they were able to inject malicious code in a library and since the library was widely used, it had a widespread impact. Because of that, we noticed that there were around 40 .SG domains that were affected. So what we did was we notified each

of the registrants for them to take the necessary action. Next slide please.

So what are the challenges that we faced when we developed this effort? Firstly, it was the education and awareness. So although we had a system to notify the registrants, we realized that some of the registrants don't know what to do with the information that we have provided to them. Also, there are times that when we looked at hosting providers, they also are unaware of the issue and also don't know what to do with the information that we have provided. Secondly, we noticed a delay in the resolution. So I think this is pretty much due to some of the registrants trying to locate their hosting providers and also partly because probably some of the hosting providers are also quite hesitant to quickly patch the issue because it may cost their other customers. And then lastly is that sometimes you have a challenge of easily taking down some of the high-risk domains. For example, there was a case where I noticed a domain with a web shell. To me, a technical guy, I feel it was quite malicious. But because it was a victim, we cannot just take down the site. So we had to notify the victim and we had to teach the victim how to quickly remove the open page. Next slide please. Okay, so what's the impact of all these strategies that we have done? Firstly, we managed to maintain a low abuse level of roughly five confirmed cases per month. Secondly, we managed to build community awareness. So based on the email notifications that our system has been sending, in a way we have created an awareness for all of the recipients of this email. And by then, they

were able to also learn how to safeguard their domain names and websites. And then third is we managed to keep the trust in .sg domain name. So at least for now, we managed to ensure that .sg remains secure and trustworthy. And then lastly, we increased the government's confidence. So basically due to the efforts that we have done on the .sg domain name space, the government entrusted .sg to also operate the SMS and their ID registry, which plays a key role in combating SMS-based scams, which we know is another realm of financial crime. Thank you.

NICK WENBAN-SMITH: Great, thanks very much. So we've got a few questions logged, but I'd like to get through Bruce's presentation first. There will be plenty of time, I think, because we're doing well, perfectly. Thank you to my panelists on the schedule. So we've got a final presentation, but start thinking about your questions. If you're in the Zoom room, feel free to drop them in. I'll try to allocate them fairly between the online participants and the in-person participants. And thanks again to Mon very much for staying up in an antisocial time zone from Singapore. Over to you, Bruce.

BRUCE TONKIN: Thank you, Nick. One thing I thought was useful in this session, I know in previous sessions, we have talked about phishing and malware, and Gabriel noted that phishing, at least internationally, is very high. We've focused on that for the last couple of years and probably seen a factor of 10 drop in the number of phishing sites

we see in .au. Mostly what's left is what we call compromised websites, where the actual website itself gets hacked with a phishing page, rather than somebody actually registering a domain name for phishing. And that's because our sort of processes at time of registration tend to eliminate most of the names that are created for phishing purposes.

What we are realizing, though, is that we're part of a wider ecosystem. And to give a context in the Australian environment, it's almost an entirely digital economy now. I mean, I go for weeks without using cash. So all the transactions are electronic. And whereas in the past, if you were scammed, it was probably down at the local drinking establishment, and someone would try and sell you something. And if it didn't work, you'd go back to the local drinking establishment and have a conversation with the person that sold you the item. In the online world, the person that's selling you or scamming you is usually not located anywhere near you. And in the Australian context, they're nearly entirely operating from outside of Australia. So it makes it difficult from a law enforcement point of view. And so the focus shifts more. It's very hard to catch the actual culprit. But what you can do is try and disrupt their activities and hope they move somewhere else. So the government focused on a scam prevention framework, which was saying that to deal with issues, you really need to look at the financial side, like how they're receiving payment. You need to look at the telecommunication side. So it's the SMS messages that get sent to the phone, which I think Gabriel said is often the start of a

scam. So you have the telecommunications companies, and then the platforms, digital platforms like social media, Facebook, etc. And you have to be working cooperatively across that ecosystem. And each person in that ecosystem has a role to play. We've now got a national anti-scam center. The government's funding that. And that's a coordination point nationally for scams. And the other activity that's interesting in our environment is gambling is very popular in Australia. And so one of the scam types is to create a gambling site where you can bet on the football and you don't ever get paid out when you win the bet because you're being scammed, basically. So I'll just put those links there just for people to be able to access some of those sites. Going to the next one.

So one thing that we have in Australia, some definitions which I thought were quite useful. A scam more generally must involve deception, and if successful, results in loss or harm to the consumer. And down the bottom, actionable scam intelligence is information that a business has that indicates possible scam activity that's on or related to their business. And that last point, I guess, is really about being part of an ecosystem that we get information from a number of sources, and we can use that information to indicate that there may be a scam happening using a domain name, and then we can take action. Next slide. So this is the framework that the Australian Government created, which I think is quite a good one, because it's basically saying these are the various steps that a reputable organization that is part of the ecosystem should take. So one is that you should have proactive

processes to help combat scams. You should have reasonable steps to prevent scams. So for us, prevention is that we do upfront verification at the time of registration. We audit registrations that come from registrars, and we audit registrations at the time of renewal to see if the companies haven't become deregistered or lost their status in the business community. We detect, which is that we need to take reasonable steps to detect activity, and I think some of that has come out this week in some of the policy development discussions in the GNSO, but bulk registrations is an example where you would look at names where a lot of names have been registered in a short period of time. They may be legitimate, but at least you should take steps to be able to identify those and investigate. Disrupt, which is taking reasonable steps, so I can identify those and investigate. So an example there is if you detect a scam, and I think I've heard a few presentations this week, is they usually do it in batches of names, and we see that. So you often realize it's one or two people running a scam at any particular time, and they're probably registering hundreds of names, and you work out what the pattern is. And once you've worked out what their pattern is, you can sort of get rid of their current batch of names. And then you have to monitor it for a few weeks, because they still don't quite get the picture, and still keep registering new names using the same previous scam. And then once you keep shutting them down or stopping them being registered, they eventually go away to somebody else in the room, another country code or top level domain. Which is also why we should be sharing information more, because I suspect once we've dealt with someone, they've

moved to someone else in this room. Then responding obviously, responding to reports. And it's that last piece that we're still trying to work through, is how do we report what we see that's actionable for other people in this room. Next slide.

Just wanted to kind of highlight the two broad types of domain name issues that we have. So one category we refer to as malicious, and this is where usually the registrant has used false information. And even though we have verification steps, if you're using stolen information, using someone's stolen driver's license, stolen passport, stolen business information, that passes most of the upfront checks. So we're finding the scammers get a lot more sophisticated and have stolen information. They've hacked somebody. You've got information from that hack from another business, and use that to register domain names. One thing we do have in our favor is we have the Australian presence requirement. I think I heard .cn China today, and Singapore, I think, the previous presentation. Because they've got rules that the domain name has to be connected to the country in some way, that can be used as a basis to detect the false information. So when we see a name that's being used for, say, a financial scam, we don't take the domain name down because there's some financial scam. We take the domain name down because they've used false information. And so we can take reports from a law enforcement agency. They don't have to sort of issue a court order. They're just saying, here's a domain name that you think, that we think might be involved in a scam. And if we look at it and see that it's got false information,

we'll take it down. And we're taking it down because they've breached our registration rules, not because of what other laws that they might have broken.

And then the second category that we see a lot of in .au is compromised websites. And a lot of business websites use sort of out-of-the-box website solutions. Some of those solutions have got mechanisms where you can write product reviews and upload content onto the website, which is a big mistake because the scammers upload content onto the website and they put links on those websites to harmful websites or harmful content. Websites get hacked, which is they're using an unpatched version, typically WordPress. And so in those situations, we don't take down the domain name because we don't want to shut down the business. We notify the registrar, they contact the registrant. And usually the registrants are very surprised that they're hosting some bad content of some sort and are usually very proactive in addressing it. There is still a user education issue because often when the registrant gets contacted, they don't even know who their hosting company is, the person that built the website left some years ago. So that often takes a while and we help them both with understanding the ecosystem, who do they need to talk to, and work with them to fix the website rather than take it down. So next slide.

So this is, I've just used the same framework as the Australian sort of scam framework, and that is at a governance level, we track all our reports and we report that to our board. We continue to tighten

our processes for validation because that's one of the preventative things we can do. We detect, so we look for, after a name has been registered, we check them. And we're looking for patterns associated with scams. So gambling sites, for example, we might do Google searches for related content and find other domains that fit that pattern and look for different sort of markers, if you like, in the registration data and take down batches of names. And that sort of feeds into that disruption, which is proactively looking for related domains. If there's one domain that's been reported by a scam, you've probably already got hundreds already in the registry, and it's finding those and sort of shutting them down. We try to be responsive and work with law enforcement agencies and encourage them to report things to us. But I'd say that the information we get from law enforcement is probably 1% less, probably much less than that. So mostly we're subscribing to a number of information feeds and threat intelligent feeds, and that's where we get our intel mostly. But we do respond to law enforcement as needed. And then the last part, which is what I'm sort of encouraging perhaps to start thinking about as a community, is how do we share information? And it's tricky because you don't want to share information that's subject to privacy law. But the more that we can share information, and as I say, I think if when we detect stuff that's unusual, that's probably happening in certainly other major gTLD and country codes as well. And certainly we support the work that the Internet Infrastructure Foundation, I think it was, that Keith's team's working on, but that sort of coordination across registrars and hosting companies. So

this is beyond just a malicious domain, but it's looking at how do we disrupt bad actors collectively. And I'll send it back to you, Nick.

NICK WENBAN-SMITH

Thanks very much, Bruce. I think across the different presentations, there's quite a lot to unpack around the fact that this is a phenomenon of huge scale and cost to our citizens who we're here to defend the interests of, and also the impact on the registry operations from both from the sort of Singaporean and Australian perspectives, just how much time and effort needs to go into it. But that time and effort, it would seem to me is still a very small fraction in terms of the infrastructure operator versus the cost to the losses still ongoing to consumers. We heard about the sort of trust and reputation being a major issue. And I think that's, as things become increasingly digitized, being able to tackle those sorts of issues so that people can, with confidence, know that who they're dealing with is actually who they think they're dealing with when it comes to goods and services and investment by its very nature doesn't, in fact, have to also be carried out online. So I know we've got some questions already, and I think Olga was first in the queue. We have got about a quarter of an hour. So over to you, Olga, but everybody else, either put your hands up in the room. I can see Hilda next. And if you're in the Zoom, put your hand up in Zoom.

OLGA CAVALLI

Thank you, Nick. Thank you very much for the presentations. I have a question for the FBI representative. I forgot your name. Sorry for that. And the amount of losses that you mentioned in your presentation, is it something informed by the victims or something that you have a method to calculate based on the damage that it's done to the victims? I was wondering if you can explain it a little bit.

GABRIEL ANDREWS

Sure. Happy to. But yeah, most of the loss figures are self-reported. So by the time that the cases progress and we move towards some sort of prosecution, obviously, we would have to validate that in order to proceed with any sort of trial. But when we're just collecting the statistics, we tend to collect the loss that's provided by the victims. But there are sometimes, just to be blunt, there are sometimes when a victim might want to exaggerate loss. You're talking about things like threats or loss to their brand image and reputation. And we don't include any of that. But things that are very tangible, like we had a ransomware attack and we were forced to pay $5 million to get access to our network again. That's pretty easy to articulate loss. Or we had a wire transfer go out and we thought it was paying one of our vendors. Turns out it was someone that compromised an email and tricked us. Those are easy to articulate. And that's where those figures, the bulk of it, comes from.

NICK WENBAN-SMITH Thank you. Should we move the slide on and move on to Hilde's question next?

HILDE THUNEM Thank you. I'm Hilde Thunem from the Norwegian Registry. I actually have two questions, but I'll start with one for FBI. At least recent research that I've seen seems to indicate that about 80% of phishing comes Now, I'm just wondering, when you deal with a case, you see that pattern, I would assume, is there a difference in how you deal with a, what is a compromised website, a compromised domain? Because then the person behind the domain is actually a victim. And you have, I would assume, do not contact the registry and ask them to take down the domain name. Hopefully.

GABRIEL ANDREWS This is a very important question. Yes, I think you're quite right that the response to the facts and circumstances that are in front of you at any given point are going to change, right? And what is the reasonable response is going to change as a result. To your point that if we, just broadly, one of the first things that you're trying to do when you're first hearing about a crime being reported to you is to figure out where the bad guy stops and ends, right? Or like where the infrastructure is actually controlled by the bad guy, or maybe is a legitimate business that he's just a customer of. And these things can take time just to figure out where that happens. And to your point, if they're using a compromised person's website, it can take

time to figure that out too. But when we're trying to mitigate harm, you're quite right that it would be a lot more reasonable if you can identify that a domain was maliciously registered to maybe ask for a registrar or registry operator to take some sort of takedown of it. But that is not at all, I would think, the go-to option for if it is a compromised site. But now you have one more victim to add to your list, right? And it may be that you need to have them be involved as a potential part of your prosecution down the road. Because in the US, at least, gaining unauthorized access to a protected computer system is a violation of US law. And so yet another crime that's occurred there.

HILDE THUNEM

Yeah. And just for a follow up for AUDA, because I really like to see that you are thinking about how to deal with compromised, which would probably be the large amount of sort of phishings and scams. But what is your experience when you try to contact somebody and tell them that their website is compromised? Because I know that as a registry, we are very invisible. And me trying to contact somebody saying that a crime is committed to try to do something would be seen as a scam. So I would definitely prefer that to be the police or the cert or somebody that, you know, people recognize instead of this strange company that says they run the internet in Norway. And they want you to do something involving your website. And you need to do it very, very quickly

because harm is being committed. And I'm ticking off all the, you know, scam boxes here. You are.

GABRIEL ANDREWS

Yes, right. Yeah, we're all nodding along. I can see this. Yeah, like we're all in violent agreement. But you're quite right. There are absolutely challenges to notifying victims. And in the past, when we've collaborated with private sector on big takedowns, and these collaborations could involve very large tech companies, they could involve internet infrastructure companies, ISPs, or, you know, companies like Microsoft. It can be sort of a balancing act trying to figure out to what extent you want to rely upon private sector to notify or where it really makes sense for law enforcement to do it. And there were occasions in the past where we thought it was reasonable for ISPs to notify their customers of, I think this might have happened in DNS cache poisoning cases. I'm trying to remember where I learned about it. But what I heard back from the case agents that worked at the time, and the ISPs they worked with, is that the customers of the ISPs actually got rather furious towards their internet service providers because they were starting to blame them for the compromise, even though they had nothing to do with it. They were just trying to take that responsible action. So I think law enforcement recognizes that there's a role to play for us to really help with the victim notification processes. It can vary from country to country, but this is absolutely part of, speaking for

myself only, not my agency, I view this as part of my role to help with. But it is a challenge and it's not easily solved, unfortunately.

NICK WENBAN-SMITH: Thank you. I've got Pierre and then Ryan Cimbolic. But first of all, Hilda, or anybody else, would you support the registry introducing legal requirements on the registrants to actually maintain basic security hygiene on their websites? And for that to be actually something that the registry...

HILDE THUNEM: No, because I don't require them to have a website. They're buying a domain name, they're buying the right of use for it to be in the database, to have a translation when somebody puts in that domain name to find an IP address. They do not need to have a website. They do not need to have email. Those are services they choose. They buy from something else. I'm not delivering them. And they are solely responsible, according to the law of electronic communications in Norway, for the use of their domain name. So me putting into the contract that they have to do certain things that I'm not part of delivering would be like also putting in the contract I'm being ridiculous, to make a point. But you need to look both ways when you cross the road and don't park where it's not allowed to park. It's a crime, but it has nothing to do with me. So no, I would not support that in our contract.

NICK WENBAN-SMITH Thank you. Pierre?

PIERRE Thank you very much, Nick. And thank you for this very interesting session, a very diverse panel. So first of all, I wanted to say that, as usual, I totally agree with .NO and with Hilde. It doesn't mean that we don't have to react when we see that there is a problem on the website. But it's different. I mean, if you put in a contract something like you have to make sure that you maintain the security of your website, the question I will ask after is, how do I enforce my own contract? How do I verify that the registrant has patched his website? So I'm not very fond of putting in a contract something that I cannot enforce.

But the question I wanted to ask the panelists, and maybe especially the panelists from the FBI, is if you can share information about the kind of discussion that you have with telephone companies. Because we are talking about the data in the Waze. Most of the scam I receive, maybe it's a specialty of France, I receive it through SMS on my iPhone. And it's not hidden numbers. They are real numbers. And I guess that the people who are sending me these kind of things didn't give their real address or their real name to the telephone operator. Otherwise, it would be too easy to catch them. So I don't know how it works. But I think that we are seeing more and more as banks or ISPs or telephone operators are asked to do the verification they are asked to do in the telecom world. And

it seems that it doesn't work either. So I would like to know, how do you deal with that? Thank you.

GABRIEL ANDREWS

I will acknowledge it's a fair question. I have to apologize. I don't have a good answer for you. I personally haven't been speaking to telco operators any time in recent memory. So I'm going to have to duck it. I will say, though, that there is across the spectrum, I think there's increasing recognition that we're going to have a society, a lot of challenges surrounding identity authentication and even authenticating that you're a real life person in the coming years. Noting how advancements, I'm going to slightly change the topic here, but noting how even tools like AI are increasingly successful in impersonating people. And the challenges of knowing that when you're talking to anyone online, how can you trust anything anymore? And I think these are challenges that we're going to have to grapple with, but I don't have solutions. And unfortunately, with telcos, yeah, there's plenty more to be said. I'm just not the right person to say it.

PIERRE

Thank you. I just wanted to add that if I did, if I asked this question, I fully understand that you're not prepared for that. But it's a way also to say that phone numbers are identifiers. No one makes the mistake. No one thinks that a phone number is content. Okay. Domain names are identifiers. So there is a true link between the two things. I think we will really should try to know how they do in

the telco industry, because we are always talking about identifiers and not content.

NICK WENBAN-SMITH: Thank you. I'll hand over just to Bruce very quickly, and then to Keith, and then we'll move on to Brian's question.

BRUCE TONKIN: Yeah, I was just going to say that that's exactly what the Australian government is trying to deal with, because each group is sort of saying it's someone else's problem, and they're saying you actually have to combine the thing, because usually it is an SMS. There is actually a bank account being paid somewhere, that's where the money's going, and there's usually a domain name as a link within the SMS message, so it's a combination. What I find interesting, for example, with the phone, because in Australia it's mostly SMS as well, but now you can report it as a scam. When you delete it, it says, is this a scam? You just say yes, but where do those reports go? I think it's trying to connect all the dots, and that's certainly what we've been trying to do in Australia, is they're starting to create registries of the phone numbers that are causing a problem, and then don't route them from one telco to another.

KEITH DRAZEK: Thank you very much for that question, and I'd just like to build on it. The Internet Infrastructure Forum, our vision as we build this out and as it evolves is to include telcos as we deal with online harms

related to smishing attacks, SMS attacks, to include the payment processors when we start talking about financial fraud. So I think the expectation is that as we have registries and registrars and web hosts and CDNs, that we're going to be continuing to add additional players who have roles in the mitigation of these harms. We all have different areas of responsibility and technical capabilities, but the coordination is really, really important, and that's one of the goals of the effort. Thanks.

NICK WENBAN-SMITH Thank you, Keith. Over to Brian. I think that's probably the last question. We've got a couple more slides, and then we'll wrap up. Thanks very much.

BRIAN CIMBOLIC Hi, this is Brian Cimbolic with Public Interest Registry. Gabe, this should be a quick question. Just on the Internet Crime Report or the Online Crime Report, one question that I anticipated follow up. Is that purely domain name related crimes, or does that include social media platforms?

GABRIEL ANDREWS It includes anything that is reported to us as Internet related crime, right? So there's a bunch of categories there, and I struggle whenever I bring this data to ICANN to try to make it relevant to you as possible. And so that's why I'm trying to highlight where there's overlap with DNS and even just how investigatively we as

investigators want to use tools that touch on DNS. But no, it goes above and beyond and probably is well more than I could talk about.

BRIAN CIMBOLIC Just briefly then, did you have any sense as far as what the breakdown was as far as the volume of social media scams versus those associated with domain names?

GABRIEL ANDREWS I wish I did, but I don't know that we categorize it to that degree of fidelity. I think already they're putting things in larger buckets like phishing, but I don't know that they're breaking down to phishing based off of smishing versus WhatsApp and chat applications versus domains. Or even if there is a phishing on SMS, did that also include a domain name within it? These are all relevant questions. I just don't think that we have that granularity in the data.

BRIAN CIMBOLIC It would be great if at some point you could, especially as this data gets presented in front of the DNS community, that break down, because my sense is that it's probably more likely to occur on social media platforms than by the DNS.

GABRIEL ANDREWS I would agree that it would be great to get greater fidelity. We'll work towards it over time.

NICK WENBAN-SMITH Thank you very much. This is a fascinating area. You can tell it's complicated. I think that's one of the purposes of having these sort of sessions, is to talk across different actors and different perspectives, because understanding the context in which some of these figures are presented, I think it's very important for us as technical operators of the infrastructure to see that we're doing it as much as we can to prevent these sorts of crimes, but also to understand where perhaps there's other places which are not really standing up and to engage those. In particular, we've talked to our government friends and policy regulators, then understanding the context and how complex it is across lots of different platforms and vectors of attack, and that this is only one element of it, and there are other areas as well, I think is a very interesting part of the discussion. So we'll just quickly move this one. We'll do the poll thing again. Let's have a little look now at the poll question. I'll call it there because it's the end of the session, but basically it's slightly changed, but not very much in the sense that there are still some areas where people don't feel their registries are well enough prepared to detect abuse, and perhaps not as well prepared as they would like to be in terms of actually managing to respond to financial crime. We heard about the complexities of compromised websites. So just finally, I just want to give a round of applause, really, to my fantastic panelists. So thank you very much.

The slide deck for completeness does include some of the resources for the desk that we can go through, and then there's a final poll for the session assessment. So I will let you do that and enjoy your coffee break. Thank you very much, everybody. Thank you.

[END OF TRANSCRIPTION]