ICANN80 | PF – ccNSO: The RA & RAA amendments what can ccTLDs learn?
Tuesday, June 11, 2024 – 13:45 to 15:00 KGL

CLAUDIA RUIZ: Hello, and welcome to The RA and RAA Amendments, What can ccTLDs learn? session. My name is Claudia Ruiz and I am joined with my colleagues, Bart Boswinkel and Joke Braeken. We 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.

During this session, questions or comments submitted in chat will only be read aloud if put in the proper form, as noted in the chat. I will read questions and comments aloud during the time set by the Chair or moderator of this session. Interpretation for this session will include English, Spanish, French, and Arabic. Click on the interpretation icon in Zoom and select the language you will speak during this session.

If you wish to speak, raise your hand in the Zoom room and once the session facilitator calls upon your name, kindly unmute your microphone. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

This session includes automated real-time transcription. Please note, the transcript is not official or authoritative. To view the real-time transcript, click on the Closed Caption button in the Zoom toolbar. To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign into the Zoom session using your full name. With that, I will now hand the floor over to session Chair, Nick Wenban-Smith. Thank you.

NICK WENBAN-SMITH: Thank you very much. Welcome everybody to what I hope will be a very informative and engaging session of the DNS Abuse Standing Committee of the ccNSO. For the record -- I've just heard the reminders -- my name is Nick Wenban-Smith. I'm the general counsel for the .UK registry, and I'm also on the ccNSO Council.

There are a couple of housekeeping parts for the meeting but, in essence, what we are going to be talking about is, in a parallel universe of gTLDs, there have been some significant changes in the past year. The first objective of this session is to make people aware of what those changes have been, but also perhaps to reflect on whether there are implications for ccTLDs. So, a simple mission, and we'll see if we manage to accomplish it.

In terms of abuse, I just want to make a couple of introductory comments, and then I will shut up. I promise. In the United Kingdom, we are having an election at the moment. In elections, people like to make grand statistical statements. For example, last week, the

conservative government said that every household in the United Kingdom would pay £2,000 more in tax if the other lot get into power.

So I thought I would copy that and say, completely boldly, that within the ccTLD community, we are lucky enough, for whatever reasons, to have 1/10-- gTLDs have 10 times more malicious registrations than ccTLDs. Ten times, that's a good, nice, round number. Unlike my political commentators, I did actually have some evidence base for this, and I did copy the figures from the most recent NetBeacon Institute report. We had a very nice session in Hamburg on tools and measurements, so we should all have at our fingertips now the right information to measure abuse in our own ccTLDs, for free, a variety of different sources and methodology used.

For whatever reason, we don't have as much abuse as is observed in gTLDs. But the gTLDs are responding and are raising their standards, and in particular, imposing new contractual obligations, not just on the registry operators of a gTLD, but more on their registrars, and I think it's the registrar side of things, which is probably more interesting for ccTLDs. I suppose in the back of my mind, I recall that in the United Kingdom, we had a slight increase in abusive registrations at about the time that the .tk domain stopped going in business. I think we all know that abuse doesn't disappear. It just moves from one place to another place. I'm wondering, well, if the gTLDs are going to get better at managing abuse, then perhaps the ccTLDs become higher up the target list.

That's one of the things that caused us to put this session on, essentially. And, you know, it's a great opportunity for all of us across the industry. Whether we're a ccTLD or a gTLD, we're still TLDs, and there's a huge unity of interest. So it's a great opportunity to build on our network of friends across the other side of the table in the gTLD world and to have a good discussion over these things.

I think, ultimately, it's in everybody's interests, in this room, not just because it's morally and legally correct but it's in everybody's business interests to make sure that there's excellent health and reputation for the whole domain industry so that it's a strong industry for everybody going forwards. I just wanted to put that on the table. I've said my bit now, and we will leave it to others.

I'm very, very pleased to have a really diverse and expert group of people to discuss these perspectives. Just to introduce people, we have at the far end, James Bladel. James, although he's a proper gTLD kind of guy, actually has a ccTLD hat as well. He was on the board of Nominet, and he's also been on the boards of other ccTLD operators. So he understands both of those perspectives as well as speaking from a big registrar perspective.

Next to him, we have Babagana from the Nigerian Communications Commission. I do think the regulatory aspects to these sorts of things are very interesting. That was something that we wanted to bring out on the panel discussion. Then we have Sam from VeriSign. Sam's here in her official role as outgoing chair, I guess, of the gTLD Registry Stakeholder Group.

Finally, but not least, we've got Adeola from Nigerian ICANN-accredited registrar, Upperlink Limited. We are going to have a moderator with Barrack from AfTLD, who is around, I'm sure, but I've not seen him here so he'll have to do a bit of catching up.

These standard slides for the DNS Abuse Standing Committee. Just a reminder that we're not here to create a policy for ccTLDs. This is about sharing information, promoting dialogue, and understanding, and best practices. Fundamentally, we want to give you, the ccTLD operators, the information and tools to be able to understand, measure, and fundamentally mitigate or prevent abuse in your TLDs. We provide a number of resources. There are QR codes to sign up to the resource library.

There is a dedicated email and contact list. I have got more propaganda, for people who need it, right here. Lots of effort is being put into giving everybody the best opportunity to fight DNS abuse. One of the things we're not going to spend any time talking about is the definition of abuse because that has been done to death. For the purposes of the contract amendments, you'll see here that the definitions are as written down on the screen. This was, I think, the work of a large number of community members and fundamentally then was adopted into the Security and Stability Advisory Committee. There's an advisory of 115, so it's the official ICANN abuse definition now. I think I'll pass it on to Sam.

SAMANTHA DEMETRIOU: This is a lot of responsibility to trust me with. Thank you so much for the introduction, Nick, and thank you to the ccNSO for inviting me to participate in this session. As Nick said, I am the current chair of the Registries Stakeholder Group, for a few more months. I will be providing some of the background, and how we went through the process and reached the decision to pursue amendments to our agreements. These DNS abuse amendments impact the Base Registry Agreement, which is the contract that the vast majority of gTLD registries operate on, as well as the Registrar Accreditation Agreement, which is the agreement that registrars who want to distribute gTLD domain names need to sign on to.

Back in early 2022, gTLD registries and registrars, a small group of us gathered for a meeting to discuss the current state of discussions around DNS abuse within the ICANN community, but also within the larger world, including some of the things we had been hearing from governments and other regulators. That was a real recognition that DNS abuse was a problem and we, as gTLD registries and registrars, had a role to play in helping to address this problem.

However, one of the things we kept hearing was that ICANN's compliance department did not have a tool to force gTLD registries or registrars to take action on DNS abuse. There was some information about abuse in our contracts, but the contracts lacked a very clear and concrete requirement to take action when you receive evidence that DNS abuse is occurring within your namespace. That was the problem that we sought to resolve.

The topic of DNS abuse is pretty wide-ranging. I think Nick just alluded to this when he talked about even just how difficult the conversation about a concrete definition of DNS abuse can be. One of the reasons we chose to pursue contract amendments was because we believed this approach would allow us to take very fast -- fast is maybe a relative term in the ICANN context -- but, fast action to start to address the very concrete problem that we faced here, which was the lack of a clear obligation in our contracts.

The idea behind pursuing the amendments was always that it would be the first step in ongoing community-driven work on the larger topic of DNS abuse, but importantly, it would establish a foundation on which we could build as a community because it would create a minimal obligation or a floor, if you will, that gTLD registries and registrars need to take action when they receive well-evidenced reports that DNS abuse is occurring on domain names under their control.

This is not a ceiling, it's not the highest standard that registries or registrars could meet, but the idea was to raise the bar and bring all of the industry up to the same minimal standard with these. Again, though, with the understanding that further work should be done in this topic and that further work should have the benefit of input from all parts of the ICANN community. This slide here, I'm going to just summarize the impact to registries that these amendments have had. I won't go into the details on registrars.

The amendments between the two are substantially similar, but there are a few light differences. The amendments require, now, that gTLD

registries must promptly take appropriate action to mitigate DNS abuse when they receive a report with actionable evidence. None of these terms that I have bolded here are defined within the amendments themselves. They are left at the discretion of the registry operator to determine. This is largely due to the fact that DNS abuse can be extremely situationally specific. What constitutes appropriate action may be different in different cases or for different types of abuse.

For the context of these amendments, we felt -- and I believe I can agree, I think I can speak for them when I say this -- that leaving the requirements a bit more open would allow for registries and registrars to take action that they saw as most appropriate, given the specifics of each individual case. We thought that was a benefit to these amendments.

What's unique on the registry side is that appropriate action for the registry may involve just referring the domain name to the registrar, for the registrar to potentially take action on the abuse. This, in large part, reflects the different roles that registries and registrars play within the gTLD space and the fact that registrars often have a more direct relationship with the registrant or the ability to contact a hosting provider if that is the better party to take action on the DNS abuse.

The last point here is, there was a slight adjustment that is hopefully going to make things a little bit easier in terms of how we receive reports of DNS abuse, which allows us to use a web form in addition to email. Email is generally how reports are received now, but web form will hopefully make some of that intake procedure a little bit easier. All of

the information, if you want to look at the language of the amendments itself, you can find that in Specification 6, Section 4 of the Base Registry Agreement.

Now that we have had the amendments approved by our stakeholder groups and taken into effect as of April of this year, April 5th, 2024, the next thing we're looking at is how to measure the impact and the effectiveness of these amendments. It's obviously very early at this point. It's only been two months. This is something that we will be working on in the months to come.

With, I think, input both from ICANN's compliance department but also from the community as a whole. I just want to share a few statistics that are available from ICANN compliance in a blog post that they published this past Friday, which is that since the amendments took effect on April 5th, compliances initiated 38 investigations with registries and registrars, which have concluded in the suspension of over 2,500 malicious domains and the disabling of 328 phishing websites.

I think one of the things that we can conclude from this is that the amendments are causing action to be taken on DNS abuse. What we don't have insight into now is how much that has changed under the amendments versus how much was happening before and the amendments are just codifying it. But I think that's another question that we're interested in getting more information about as we go forward, again, in coordination with ICANN's compliance team.

Hopefully, this provides a bit of a scene-setting about what the amendments cover, how we got here, and why we chose amendments

versus a different process such as policy development within the GNSO. I'm happy to take any questions about it or pass on to the next speaker.

NICK WENBAN-SMITH: Thanks, Sam. That was very clear. I think there's no need for questions because it was so clearly explained. Thank you very much for that. I mean, I've got lots of questions like, why do you need to have a contract requirement in order to do something which is the right thing to do? I think that's a different philosophical discussion, maybe for later on. Similarly, whether this is fast enough, or whether these phishing and registrations would have been dealt with anyway without the contract amendments. It's hard to measure that sort of thing. I think we'll move on now to hear a bit more from registrars, who have got the sharp end of the stick in terms of contractual requirements and ICANN compliance on their case. I'll hand over first to James and then to Adeola.

JAMES BLADEL: Thank you, Nick, and thank you, Sam. I'm James Bladel. I am the VP of Government and Industry Affairs for GoDaddy. As Nick mentioned, we're also very involved with the ccTLD space, both in partnership and in our direct involvement with country codes like .me (Montenegro). I don't know if they're in the room. Very grateful to have some time in front of the ccNSO and to share some of our experiences thus far with the new DNS abuse contract amendments, which as Sam mentioned, have only been in effect for a couple of months now.

I think the first question, and one of the more common ones that I get, is why would registrars voluntarily agree to adopt more stringent obligations under their contracts? And I think there are a few good reasons. This goes to Nick's question as well, what's in it for us to agree to new contract amendments? The first one is that, of course, DNS abuse is an industry-wide problem and requires a coordinated industry approach to solving it. There's only so much a registrar with the best of intentions can do, even a large registrar, to move the needle on this particular problem. It's always best to work as a coordinated industry.

Secondly, some registrars have made significant investments in technology and people and toolkits to build the capabilities to detect and mitigate DNS abuse. In a way, we were at a competitive disadvantage to those registrars who weren't being as responsible or aggressive in this area. So, agreeing to contract amendments would, in effect, set a standard, set a floor as Sam mentioned, and help level the competitive playing field in that regard.

Then finally, registrars, particularly those that regularly attend ICANN, are committed to the self-regulation model and would much rather have a participatory approach to these types of problems than have them handed to us, either within ICANN or, unfortunately, externally through legislation.

One of the big wins, and I think Sam touched on this as well, is that having standardized definitions for what is in scope of DNS abuse and what is not is a big part of what we took away from this exercise. I think folks who have been at ICANN for an extended period of time know that

definitions are important and sometimes can consume more than half of the work when writing a new policy.

What's new? I think Sam summarized very well, but from our perspective, registrars now have an affirmative obligation to investigate DNS abuse reports, and if they're detected, to take steps to disrupt any DNS abuse on their platform. ICANN is now empowered to oversee those processes and ensure that registrars who are not making an effort to comply with these new agreements are subject to the same compliance framework that they would be if they had any other policy or contractual violation.

It's important to note that, going back to the definitions, the amendments do not cover other categories of abuse, like content issues or IP infringement. Wanting to note as well, that goes back to the idea that the definitions are very important. It was very critical for us to draw a line around what was and what was not considered under the umbrella of this particular problem.

As Sam mentioned, these are fairly new. The amendments took effect on the 5th of April. We are still in a data-gathering and fact-finding mode to understand exactly what sort of impact these may have had on the problem. The good news is, for many registrars, these new rules did not or should not have required significant changes to their existing abuse detection and mitigation practices. We had engaged in a previous exercise, the framework on DNS abuse, which was an opt-in voluntary industry effort to define and coordinate anti-abuse efforts. Much of that framework was incorporated into this work in amending

our contracts. In effect, registrars and registries who participated in that development of that DNS abuse framework had a head start in complying with the new contract requirements.

There is, however, still an open question, a bit of a wild card on whether or not the volume of reports will increase. That includes the volume of reports that registrars would normally receive. It includes the volume of complaints that might be delivered to ICANN in terms of enforcing the new agreements. We're still early days. It's only been two months, but we are monitoring very closely to ensure that we are getting the appropriate level of quality and quantity of reports.

Sam mentioned in her slides that we also created the ability for registrars to accept reports via web form instead of just email. Previously, email was the only allowable mechanism for receiving reports. Having reports submitted through a web form gives us a significantly better ability to capture, track, categorize, and route those reports to the appropriate teams internally. That's essential for a large service provider that's dealing with a high volume of reports.

Here's the story so far. I still call it, sometimes, the DNS Abuse Institute, but it is rebranded as NetBeacon, providing registries and registrars and others with reports and performance metrics that will provide a snapshot of where our DNS abuse picture was prior to the new amendments and as we go forward with these new practices, and gives us the ability to measure the difference that we're making. Additionally, they will identify which contracted parties are making a good-faith and concerted effort to live up to the new agreements and which ones are

falling short of those new obligations. I think this is important. I think it was Sam that mentioned that there's not a one-size-fits-all to DNS abuse because it's very diverse in the way that it presents itself.

NetBeacon can also demonstrate the different categories of abuse, for example, new registrations versus compromised websites. I can share that in some cases, a large registrar may have a disproportionately large number of abusive domain names that were newly registered whereas another large registrar may have most of their DNS abuse occurring in domain names that have been registered for many years but have been compromised in some way. Maybe it's a hosting package or WordPress blog that has been compromised and is now being used for abuse. That's an important insight to get from NetBeacon. It's a great tool.

I think that there is still a lot to be learned in terms of how ICANN is going to be responding to the new rules. As I mentioned, they're now receiving reports. There were some good statistics in the blog post on Friday. The volume of reports seems to be higher, at least initially, but ICANN is also looking at some of the-- I don't want to say pre-screening, but they are examining some of those reports to determine whether or not they are appropriate to forward on to the registrar.

One of the things that we are seeing very commonly is that someone reporting DNS abuse will simultaneously report the abuse to the registrar and to ICANN at the same time. That's not helpful. ICANN's role is not to be the oversight of the registrar process. They are meant to be in place if the registrar fails to respond or fails to investigate or just doesn't take the appropriate next steps. Sending those reports to both

parties simultaneously is, let's say, a misunderstanding of how the roles and responsibilities play off of each other.

Then, of course, anything that is incomplete, contains insufficient data, or is just not complete enough to conduct an investigation is also being rejected. ICANN has also mentioned that they're focusing on, at this moment in time, at the early point, focusing on systemic failures and not necessarily single incident abuse reports. I should mention that they're having a session with registrars concurrent to this one. I skipped out of that session to come here but, hopefully, they're covering some of these things and perhaps even sharing some new information as we go.

Finally, I'm just throwing out some ideas for ccNSOs. I know that everyone is taking this on board to see how much of it is appropriate for their TLD, but some thoughts to keep in mind is aligning standardization of DNS abuse wherever possible is always going to be beneficial to the registry and registrar universe. New policies aligning with the gTLD contracts will ensure that your registrars are almost always automatically compliant with any new rules that would be adopted. These were subject to a lot of discussion and analysis, so there's no need to reinvent this from scratch. You can borrow these.

We encourage the ccNSOs to borrow heavily from this work if they choose to do so. Particularly with the terminology and definitions, so that when you're communicating to your registrars, you are speaking the same language that they are speaking with each other, with the registries, and with ICANN. It's good to standardize that terminology.

Trusting the registrar's decisions, I noted that overly-prescriptive policies or requirements are usually a benefit to the threat actors who are seeking to conduct abuse, because it spells out the pathway for them to circumvent detection mechanisms and abuse and mitigation mechanisms. So it's always good to allow some degree of discretion to the registrars to conduct the investigation and decide what the most appropriate action is, and that is something that we reserved in these new contract amendments was some degree of registrar discretion.

Talk to registrars. Some of them may have a lot of expertise in this area. I know I mentioned it several times to Sam and her registry colleagues but, the registrars are on the front line of this particular issue. The registries are maybe one step back. There is a lot of experience and expertise to be gained from the registrar community in dealing with DNS abuse.

Then finally, there's always room for more on this boat of registries, registrars, country code operators, and ICANN working together to address this industry-wide problem. I think we can go back to something that Nick mentioned in his opening remarks is that abuse never goes away, it just moves to the most vulnerable parts of the internet and the domain name system, and we can continue to make that a smaller and smaller and more marginal part of our industry and the remainder of the gTLD space and the ccTLD space will become more trusted and more free of abuse as a result. I think that's the end. Thank you. I appreciate your slides. I think you're next.

NICK WENBAN-SMITH: Thank you very much, James. Very clear. Dr. Eberhard.

EBERHARD LISSE: I have a question. Have you got any registrars who act differently on different TLDs? In other words, if a registrar is in compliance with gTLDs, could it be that they're not in compliance with ccTLDs? Because it's all automated. I would accept all the registrars that are in compliance where there are no justified complaints or sustained complaints, the ccTLDs shouldn't need to worry because they are all in compliance.

JAMES BLADEL: That's possible. I could see where a registrar might just-- it would be easier and less expensive to apply their gTLD practices to all of the ccTLDs that they also support in their business. I don't know that we should assume that would be the case for all of them, but it certainly seems to be a rational decision that registrars would do that. The goal is to continue to level-set for the entire industry. Therefore, I think if it was a policy or a contract change, or even just a communication from the ccNSO operator to its registrars, "We expect you to take the same practices that you are now required to deliver in gTLD space and treat the ccTLDs similarly," even that would be acceptable as that messaging was clear.

NICK WENBAN-SMITH: Thanks very much. I've also got Kristian.

KRISTIAN ØRMEN: Thank you. Kristian from the Swedish Internet Foundation. It's not really a question, more of a comment. I just wanted to say that as a TLD to work with your registrars on fighting abuse is a million times more effective than trying to do it yourself, so I can just add to what James was already saying.

JAMES BLADEL: Thank you, Kristian.

NICK WENBAN-SMITH: Brilliant. I don't see any more hands in the Zoom. I see Pierre.

PIERRE BONIS: Not in Zoom, thank you. I'll speak in English because I'm not very sure that the high table is with a handset. Oh yes, so I'm going to switch to French. Great, thank you. [Participant speaking in French]

Okay, I'm going to switch to English if you don't have the translation, otherwise, it's going to be difficult. I just wanted to know, from your point of view, if the change in the contracts in ICANN gave you the power to do something. Because we always talk about the new obligations that are in the contracts but sometimes, when we have this relationship with our registrars and ask for them to act, they answer us that they don't have this power.

Is it something that, because it's written in the contract, allows you to do something that you were not able to do before? Or it's just a new compliance policy to put in place? Thank you. The question is for the registrars, from my point of view as a registry, but it goes also for the registries that didn't have the opportunity or the right to act upon several domain names before.

JAMES BLADEL: Sure. Just very briefly, the types of abuse that we've defined in our new contract have already been prohibited by our terms of service and our domain registration agreements. In that regard, for my company, no, it did not. We always had the ability and have had the ability to act on these reports. I think what it does is maybe for the registrars who hadn't had those very explicitly prohibited by their domain registration now must act on them, and then one would assume they have to go back and amend those agreements to make sure their customers are clear that if you're engaging in these abusive activities we will suspend your service under your agreement. For us, no. No change.

SAMANTHA DEMETRIOU: On the registry side, I think it's very similar. The amendments didn't grant new powers or permissions for registries to take different kinds of actions. I think one important thing that they captured was that a valid response to DNS abuse would be to send it to the registrar. Then having the similar requirement in the registrar accreditation agreement, I think provides maybe a bit more assurance that action then gets taken to

mitigate the DNS abuse that maybe wasn't solidified before the amendments were in place.

NICK WENBAN-SMITH: Great, thank you. I wish to move on. As the qualified lawyer on the panel, it's quite one thing to have a contractual clause, it's another thing to enforce it. I think it's the obligation to act, which is the interesting point here as there is a specific obligation to act where you have things which merit it. I suppose the other point is that we know that a lot of abuse is concentrated in relatively small pockets. It enables compliance to target those. Without any more ado, I wanted to hand over to Adeola, because we are obviously in beautiful Kigali so it would be wrong of us not to have a really interesting insight from the African region. Thank you.

ADEOLA RAJI**:** Hello, everyone. Good afternoon. My name is Adeola. I work with Upperlink Limited in Nigeria. Thank you so much for this opportunity. DNA abuse has been a thing since forever. In 2020, that's during COVID, the rate at which people registered domains went up by 200%, and so is DNA abuse. In a day, we receive nothing less than five complaints. I know it will be worse on bigger registrar end, and different kinds of complaints. We are not the only ones, not only the registrants, not only the public, they target registrars, they target our server.

When the amendment came in for us to vote, we were glad to say yes to it. We said yes without even hesitating because when we went through

it, it has a lot of good impacts. Number one, the idea is to control the internet, to make the internet safe, the ecosystem safe for everyone. And then also, to control what is going on out there. There are a lot of things, there are a lot of people that just want to go out there, take people's money, scam others. Without wasting too much of your time, I'm just going to go into my points.

I'm going to be talking about the impact of DNA abuse on registrar business from Africa registrar perspective. Based on the amendment, I have some points here, but I won't be saying much since Sam and James has covered a lot. My slides highlighted the 2013 registrar policy and 2023 amendments. I'm going to assume we all know it so that I won't waste too much of your time. Why this discussion matters? It matters because we want to make the internet safe for everyone.

The aim is to combat the increasing stances of DNA abuse, such as phishing, malware, distribution, botnet, pharming, spamming. I think there are other ones, probably that will be coming under country code. We have what they call pig butchering, that's cryptocurrency, although it is not certainly the DNA abuse. Then I'm going to be talking about the impact of the amendments on registrar business, the challenges, and how country code can be of help in combating the DNS abuse.

From my perspective, the amendment takes care of tracking and accountability in the sense that it says it clearly that, "Registrar, you are to do this..." unlike the one in the registrar accreditation agreement. You are to acknowledge every complaint received, and doing so, it makes it easy on the registrar end to track every report received. It also

improved complainant and accessibility in the sense that, if there is a complaint about abuse, you can easily go to their platform.

We have a web form. A lot of people don't know. If I'm not in the industry, I wouldn't know that I need to go to Abuse at www.upperlink.ng. I don't know the policy states that every registrar must have an abuse email. But by doing so, having a web from and a platform, it makes it easy on registrants and user end to easily complain about DNA abuse. And by doing so, we are reducing the rate at which people are committing crimes on internet space.

It also protects SMEs in the sense that it's stated clearly in this agreement that when there is a complaint about an abuse, registrar to investigate. We are talking about subdomains, second-level domains. You have to check, contact the registrar that, "Okay, this domain name, there's phishing going on on this. Can you take down the phishing content?"

There was a customer that had an issue, and this was an issue with a big company. We established that this person is running a legitimate business in Nigeria, established business, but because they feel he's here, they are there, and also the kind of content, so the registrar suspended the domain name and the hosting was canceled. We were able to provide all the necessary documents. So with this amendment, it makes it easy for the end user to provide evidence in mitigating abuse, and collaboration with stakeholders. It also promotes stakeholder engagement.

My company is part of a registrars stakeholder group and I'm also part of DNA abuse group. We share a lot of things in terms of the action to be taken, taking proactive measures, and also the ability to spot patterns. These are the things that this new amendment also promotes, and it also reduces legal conflicts. If there is a complaint, it is mandated for every registrar to take action. You are not just to receive the complaint. Receive, acknowledge, and take action accordingly that depends on the severity of the complaint.

If it's something simple that you can settle within a couple of minutes or an hour, 24 hours, do it. If it's not, acknowledge, and make sure you do the proper thing. In doing so, there will be a reduction in court cases, because you know that when you send an email, there's definitely going to be feedback on the mail. In essence, the new amendment modification will improve registrar tracking accountability. It will make it easier to comply with ICANN requests. It will also increase reporter's access and reduce illegal issues, and these are the positive impacts of the amendments.

How ccTLD can help combat NSS abuse? I'm from Nigeria, we have NERA. They are doing a wonderful job. I can attest to that. There was a time we had an issue with law enforcement. There was an abuse case, they just barged into our own company, my superior. They arrested about three people because of something we don't know about. Then NERA came in. They set up a board. The purpose of the board was just to enlighten law enforcement agencies, let them understand the abuse case, how to investigate, who to contact when there's an abuse. Since they did that, they stopped harassing us, they stopped harassing every

registrar. When there's a case, they know who to contact. These are things that every country code ccTLD can imbibe if it's not yet in place.

Also, by having a clear rule. Clear rule in the sense that it's clear-- to make it easy for them to support and stop abuse. When it is in place, they know what to do. And also, checking registration. For registrars, the country code also help by always checking registration, easy reporting. They can also imbibe what we have in gTLD. You must have a form on your page. Have a form, have an email. It's not only registrar. A lot of people don't know registrar, but in my country, some know NERA. When there's an issue, instead of them to go to registrar, they went straight to registry. When the registry also has the same place, when complaints come in, instead of it goes to them, it comes to us. And they always find a way to manage the two sides.

Also, educating registrants and law enforcement agencies about DNA abuse best practices for prevention and reporting. A lot of end users don't know what abuse is. If I'm not in the industry, if I receive an email that you have to click on this, I'll gladly click on it. And this might cause an issue on my end. There are a lot of users that don't know about this. Some do know that there are emails that the pirate have a regional domain name and they are actually fake. Some will register.

This is a pattern I noticed. Let's say, banks. Instead of them to have www.bank.com, they have www.bank.ng.com. If you are not sure of which URL you're clicking, you'll go to www.bank.ng.com and you will provide your information. At the end of the day you will realize. By the

time you realize that you have been scammed, it's most likely too late. And such people, they don't know who to contact.

Registrar can come in here to educate end users on what to do when they spot an abuse and when they see something different from what they should. Collaboration with law enforcement agencies to detect, investigate, and prevent DNA abuse effectively. Working with DNA law enforcement agencies is also a big deal. We usually receive an email from different countries' police. They send an email, "There's an abuse case," and we're always required to provide information.

We are always willing to help because we know the purpose of their request. These are also things that the registry can come on board and educate law enforcement agencies better. "When there is this kind of case, this is what you need to do... These are the actions that need to be taken..." Also, working with registrars to ensure everyone follows.

Some registrars feel they are registering the domain names as long as the domain goes through. We don't check the process. These are the things that the registry also needs to put in place. I feel the registries country code should imbibe gTLD policy. Having a uniform policy actually access on registrar end, we are picking gTLD policy, we are picking country code policy, and we also have other policies to pick from in terms of DNA abuse. Having a centralized DNA abuse policy, it's up to both sides, both the registrar and the registry. Thank you.

NICK WENBAN-SMITH: Thank you very much. There's a lot of good practical advice in there. I think it's quite interesting, as a registry, to be told in no uncertain terms by registrars, basically, there are certain things that registrars are better at. That's the appropriate way to deal with it. Just a nice segue into the regulatory side of things, because I think as James said, the reason why we prefer the self-regulating model is that we can pick something which is flexible and good for the industry without having it being imposed on us. I am interested in regulators.

I've got Babagana here from the Nigerian Commission. How bad does a problem need to be before regulators decide that they need to intervene? Because I think that's what we need to make sure that we avoid.

ENGR BABAGANA DIGIMA: Thank you very much, Nick. My name is Engr Babagana. I'm from the Nigerian Communications Commission. As Nick has said, he has laid down a marker at the beginning that we don't have to define what is DNS abuse. I also want to say that as regulator, we are government, and my perspective here is from that point of view, and on amendments. To give a context, the background is that these amendments to the gTLD Registrar Accreditation Agreements introduce enhanced measures that we think will mitigate DNS abuse.

We're also in agreement that these amendments are critical also for the ccTLD managers as they establish global baseline for anti-abuse efforts. We also agree, of course, that the amendments will bring in a more

secure and abuse-resistant internet, and it will signify the need for regulatory alignment and proactive engagement.

From our own point of view, we look at it from what impact will it have on Nigerian citizens in particular. And we feel that it will bring improved online safety. Of course, we have a lot of concerns or a lot of reports, especially for abuse emails that are originating from Nigeria, for instance, scams and so on. We feel that this improvement will bring down that sort of abuse. We also feel that it will strengthen our own infrastructure. For instance, the .ng will benefit a lot from measures because it will improve our image as Nigerians in the digital space. We feel also it will give local support to companies that solely rely on the .ng.

I will still talk about the DNS abuse itself, even though Nick has mentioned that we don't need to define it. As Nigerians, as regulators, and as government, we still feel there are some forms of abuses that should be defined or categorized as DNS abuse. For instance, in recent times, Nigeria has been facing a lot of challenges with websites that undertake business activities in Nigeria that they are not licensed to, things that we have clearly marked as illegal.

In particular, we have issues with cryptocurrency exchanges that are being used as a platform for value discovery in Nigeria. This has been an effort that we feel ICANN will have to look at it and see it as a form of abuse. If we define a licensable activity in Nigeria, for instance, and then you, DNS, you're using your website to undertake activity without those licenses, I think we feel that should be part of what constitutes DNS

abuse as well. We may keep this for a later discussion, or we'll wait for the next amendment to take effect.

Then the next thing is, what are the challenges that we face as regulators? Of course, anytime there are changes to whatever form of change, we also expect some challenges. The simplest of the challenges, of course, how do we bring awareness to these changes for our registrars and ccTLDs and so on? So we need to push that as one of the challenges. These are things that we are taking care of in some of our plans already.

Of course, we also need to bring alignment to our regulations, to our guidelines that we have that are existing. So we need to make changes to those. We'll also talk about capacity building. I will keep this for the next bullet point. Then of course, there are some technical adaptations that need to be undertaken by the registrars, for instance, about the RDAP and the rest.

For ccTLD managers, again, we see the necessity to balance international standards with our local realities. What are our local realities? And that's why I say we keep the capacity building. You see, Nigeria, like most developing countries, has been faced with a lot of challenges, especially as regards movement of skilled labor. That's where we have this fish that is jumping from one pot to another.

There's a term we call "japa" in Nigeria. It's something that has been very much a challenge to us because a lot of our skilled people have been moving, especially in IT. The network engineers and so on have moved away from Nigeria in the past two, three years, to other

developed countries. That is a challenge because all the people that we have that are trained, that are skilled in implementing network operations, especially in implementing DNSSEC, for example.

Some of the operators we spoke with has said one of the challenges they are facing is not the implementation itself, but because the people that will implement and run the network and do operations and so on, move. After a year or two, they move from the company and then they are left with a network that they can hardly manage. They don't want to add that layer of complexity. This is the similar challenge that I feel the implementation of these recent changes may bring. It's not only in DNSSEC but also in this area.

For us, we feel those local realities, which we can put in perspective-- There's a bank in Nigeria that lost 80% of its IT staff within one year. That is a challenge because it's similar across all other IT-related fields in Nigeria. We feel that the ICANN board will have to look at the issue of training and capacity building, and developing skills. We cannot stop people from going to other places, but then we need to replenish what has been lost. I think this is one key challenge that we feel ICANN should take and look at it critically, continue training Nigerians and other nationals, especially from Africa.

We also go to what is our role as regulators. Like I've mentioned earlier, we need to look at our rules, our regulations, our guidelines, and see how we evolve with these recent changes. One of the key things that we are looking at currently in Nigeria is how to bring out a guideline for internet governance and for cybersecurity.

One of the things we do is, of course, we will have to adopt industry standards that the industry has set. We will look at the recent changes that we are having currently and we'll adapt it to our own local scenario. At present, we are at the review stage. We will next go to consultation with all the players, the industry players, then we will have a draft, hopefully by the end of this year or early next year. We'll look at alignment with ICANN standards and also enhance our own ccTLD reputations as well.

Collaboration is still part of the things that we are talking about. Adeola mentioned law enforcement that has visited our office. We are also in similar situations, but we work, as a government, with law enforcement. We also work with the civil society and private sector. The need for that collaboration to exist, it's paramount. Because all the changes, most of the law enforcement agencies, unfortunately, do not have the background or the insight to what is happening, which takes us back again to the point we are making that we need to inform the stakeholders. The stakeholders are not only the people in IT, but also the people in law enforcement in the private sector and so on. So this is one key area that we are looking at as regulators to involve everybody within our sphere.

For the NCC and for Nigeria in general, in the future we're looking at review of our amendments. I've have mentioned developing new guidelines and regulations that will align with ICANN's policy. We're also looking at stakeholder engagement. Aside this, we're also looking to plan and adopt advanced technological tools for real-time abuse monitoring to enhance our framework, to include specific provisions

against DNS abuse, and foster international cooperation. In conclusion, as regulators, we are committed to adopting and advocating for and adapting to these global standards, safeguarding the .ng domain name in particular, and ensuring it stands as a beacon of trust and security in the digital world. Thank you.

NICK WENBAN-SMITH: Thank you very much. That's the end of the PowerPoints, you'll be pleased to hear. This is now a question for more panel discussion. I would like this to be a two-way thing. I'll hand it over to my friend, Barrack, to moderate the discussion. If there's anything you want to ask any of the panelists, or just comments or observations around this important topic, then we have 10 minutes. We have a very prompt hard stop for those of us going to the genocide memorial visit after this so let's make the most of the time now. Thank you. Barrack?

BARRACK OTIENO: Thank you very much, Nick. Do we have any questions from the floor directed towards our panelists? Yes, please.

IRINA DANELIA: Thank you, Barrack. It's not a question, but it's more a comment, if I may. My name is Irina Danelia, and I am with .ru country code for Russia. We have been running for 10 years a project that allows us to detect and suspend malicious domain names, which involves expert organizations and registrars and registries, definitely. In the last year,

it was about 460,000 domain names suspended with this project, and it's 5,000 domain names per month this year.

Having such a big volume and also attempting to reduce the time from the case identified until the domain name suspension to reduce this time of reaction. You cannot 100% guarantee the mistake and false positive situation. Statistically, one false positive, one legitimate domain name out of 50,000 is almost zero. Practically, there could be a situation where a chain of human mistakes, even in a very well-sought and duly arranged process, leads to a legitimate domain name being suspended by mistake.

If this happens to be a domain name of, let's say, a big bank or a big marketplace, the reputational and financial damage for the registrar can be significant. I would definitely welcome the discussion on what safeguards could be built in the processes to avoid or reduce the risk of such a situation. Maybe not for today, maybe for future meetings. Thank you.

BARRACK OTIENO: Thank you very much, Irina. Any other comments from the floor? All right, before I move back to the audience-- Please, go ahead.

ALAN WOODS: Hello, everyone. This is Alan Woods from CleanDNS speaking. I suppose, just following on from what was said from the last speaker there, I think one of the good things that we can see as perhaps a good synergy between the ccNSO and the GNSO's response to this is ensuring

that there are very clear statements and principles. I think what comes through on the new gTLD amendments are things such as ensuring that there are standards of evidence, that there are clear thresholds that we're all coming from.

Now, the DNS abuse amendments, specifically, were with relation to the minimum expectation, but also having these clear standards of evidence, having these clear standards of thresholds, importing and imparting a necessity as to non-arbitrary action. These are things which I think are very core and where I think both the gTLDs and the ccTLDs can be aligned. It definitely would be encouraging, starting from those principles where we are aligned, and absolutely seeing where we can build from there to prevent false negatives. To prevent false positives and ensuring that we're doing the work in a measurable manner, I would suggest starting with those very clear unifying principles.

BARRACK OTIENO: Thank you very much. I don't know if any of the panelists want to respond to the comments. Please go ahead.

SAMANTHA DEMETRIOU: Thank you. Thanks for the contribution, Alan. I want to just note a bit of a programming note, which is that on Thursday here in Kigali, the GNSO Registry and Registrar Working Groups on DNS Abuse will be holding a workshop, which is a cross-community workshop. Everyone is invited to attend. One of the topics that they will be discussing is something Alan just mentioned, which is effective abuse-reporting. I

think that in the spirit of having some industry-wide standards, having more voices and as many ccTLD voices who would like to be present for that and contribute to those discussions would be very valuable. So I would just extend the invitation for everyone to attend that session.

BARRACK OTIENO: Thank you very much. Any of the panelists who want to respond to the questions that have been raised before I turn back to the floor? No? Any other takers from the floor? As I wait for the questions to come through, as we prepared for the session, we did a desk survey. Actually, earlier on, there was a similar conversation in the GAC. We did a random desk survey at AfTLD for 12 ccTLDs in Africa.

Some of the questions included some of the most common forms of DNS abuse that they encountered. The majority of them indicated that it was phishing, for instance. Another question was whether at all they consider DNS abuse as a significant issue that needs more attention. And 100% of all the 12 respondents from all the sub-regions indicated, "Yes." I don't know, as I bring this back to the floor, whether we have any more queries or more concerns. Yes, Joke?

JOKE BRAEKEN: There's a question in the chat saying, "The statistics given on compliance reports from April 5th, 2024, are they to be understood that ICANN Compliance instructed registrars to suspend 2,528 malicious domain names?"

BARRACK OTIENO: Thank you, Joke. Anyone on the panel who wants to speak to that?

JAMES BLADEL: I would say that the verb is not correct. ICANN doesn't instruct registrars to suspend domain names, but it would ask or confirm that a domain name was suspended by the registrar as part of the investigation of the DNS abuse report. I'm not sure if I'm answering that question correctly, but I wouldn't say that ICANN is not directing the outcome of those investigations or requiring registrars to take specific actions, only monitoring that they are investigating and taking the action that they determine is appropriate.

BARRACK OTIENO: Thank you. I think with that, I'll just take a round of closing remarks and hand over back to Nick, seeing no further questions from the audience. Starting with James, your parting comments?

JAMES BLADEL: No. In the interest of brevity, I think it was a great session. Thank you, again, for including us. Thank you for thinking that there are some learnings to be shared across the gTLD and ccTLD space. I think that the more that we can be aligned, the better we can be more effective in cleaning up DNS abuse across the domain name system. Because the abusive parties don't care, gTLDs or ccTLDs. They just want a domain name that works so they can conduct their threat campaigns. And so, we can work together to disrupt that.

BARRACK OTIENO: Thank you. Babagana?

ENGR BABAGANA DIGIMA: Thank you. I think I also align with him regarding the abuse, but I'll also reiterate the fact that abuses are things that are of interest to we as a government. For the image of our country, we also need to show that we have done something to minimize abuse, either originating from Nigeria or from other territories. We also want to be sure that the global community is also helping in that regard. Thank you.

BARRACK OTIENO: Thank you. Sam? Kindly be brief.

SAMANTHA DEMETRIOU: Thank you. Just to say that further work on DNS abuse beyond these amendments is ongoing and will benefit from diverse community input. We look forward to working together on it going forward. Thank you again for having us.

BARRACK OTIENO: Thank you. Finally, Adeola.

ADEOLA RAJI: Thank you. Thank you, everyone. So far, it has been a great session. I'm sure Upperlink, my company, and everyone, we are going to work

hard to make sure we do our part in combating the DNS abuse and also to mitigate it and take action when there's a report on the DNS abuse. Thank you.

BARRACK OTIENO: Thank you. And back to you, Nick.

NICK WENBAN-SMITH: Well, that was a very interesting and far-reaching session. I want to give a massive thank you to all of the participants, everybody who's engaged, everybody who's attended and given the matter some thought. It is a really important subject. It's obviously an ongoing discussion. It's high interest in respective governments, which is very important for ccTLDs. Phishing is probably the major problem, I think, that we all see in terms of malicious registrations that is fairly and squarely caught by the contract clauses we're talking about. So, there couldn't be nothing more topical. I'd just like to finish with a big thank you and a round of applause. Thank you.

[END OF TRANSCRIPTION]