ICANN76 | CF – GNSO: CPH DNS Abuse Outreach
Monday, March 13, 2023 – 13:15 to 14:30 CUN

SUE SCHULER: Hello and welcome to the CPH DNS Abuse Community Outreach 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 the session. If you would like to ask your questions or make comments verbally, please raise your hand. when called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking. The session includes automated real time transcription. Please note this transcript is not official or authoritative.

To view the real time transcription, click on the closed caption button in the Zoom toolbar. To ensure transparency of participation in ICANN's multistakeholder model, we ask that you sign into the Zoom sessions using your full name. For example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name. With that, I will hand the floor over to Brian and Reg.

BRIAN CIMBOLIC: Thank you, Sue. Hi everyone. My name is Brian Cimbolic. I am one of the co-chairs of the Registry Stakeholder Abuse Working Groups. And I along with Reg Levy here from Tucows, one of the chairs of the Registrar Stakeholder Group Abuse Working Groups will be chairing today. So can we go to the next slide.

Next slide. So today on the agenda, we are going to give a brief update on the DNS Abuse amendment both on the RA and the RAA, and Owen and Chris will be walking us through that. And we will also-- Ashley Heineman and Alan Woods will be giving an update on responses to the letters sent from the GNSO relating to DNS Abuse.

REG LEVY: After that, Alan from the Registry Stakeholder Group will be giving an overview of personal data management in a way that is privacy forward. I will present on the ACID Tool which is a wonderful tool created by the Registrar Stakeholder Group. And then I will turn it back over to Owen for AGP limits proposal, the Add Grace Period limits, and then he will turn it over to Graham and Rowena from the DNS AI.

BRIAN CIMBOLIC: And with that, we can hand things over to Owen and Chris to give an update on the abuse amendments.

OWEN SMIGELSKI: Thank you, Brian. This is Owens Smigelski. I am vice chair for Policy Registrar Stakeholder Group with the registrar Name Cheap. And

along with Katherine Verdaguer, I am the co-chair of the DNS RAA negotiation team for DNS Abuse Amendment. So we kicked us off back in December, the registrars and the registries initiated this contract negotiation. And it's my understanding, this is the first time that the registrars and registries have done so, it's always been ICANN has done that.

And we did so because with all of the abuse activities that are ongoing, which you will see here, as well as in other areas of the community, in part from what we saw with the GNSO Council small team on this is that there is actually more action that can be taken. So what we want to do was to do something that could be quick and effective. It may not necessarily solve all DNS Abuse, but we do hope that this will make a meaningful impact. And while ICANN processes are good, and we support the multi stakeholder model, as we all know, sometimes it can be measured in years as opposed to months.

I'm sorry, I will get closer to the mic. And so it's our hope and intention that these negotiations can be concluded within the year of the trigger, which was in December. And we do expect that there will be a red line draft shared publicly for a public comment period, and this should happen we anticipate prior to ICANN77. And so what we want to do through these negotiations is to establish some meaningful baseline obligations in each of the agreements that will require contracted parties to take reasonable and appropriate action just to disrupt and or mitigate DNS Abuse, and thus allow ICANN Compliance to enforce this accordingly.

I speak for the RAA, currently it states that it requires you to-- a registrar to respond to an abuse complaints, and in theory, sending an email response saying, we've received your complaint is sufficient under that wording. So what we want to do is make sure that there are clear cut actions that are required there to stop this DNS Abuse. So the things we're focusing on are what is a generally accepted within the ICANN community through the SSAC of ICANN on their website, which is there are five, excuse me, four types of DNS abuse, phishing, farming, malware, botnets, and then a fifth, spam, when used to deliver any of the other four.

So this, these negotiations are not focusing on content, they're not talking about spam, that's separate from those other four types of abuse, and is also not going to be focusing on registration data accuracy. But the goal is we want to make the obligation for a registrar registry to have to take action when abuse is reported that's within the scope.

To do so, we want to make sure we can specify a reasonable-- I guess I'm too close there-- achievable and enforceable obligations. Like I said before, there's not really that there, so this will specify things that registrars need to do, and may vary based upon the business model, and then also, within the responsibility of that contracted party. What this is going to do is it's going to establish a floor not a ceiling, meaning that all registrars and registries will have to do this minimum because right now, not all of them have to do so.

And so this will allow Compliance to hold all registrars and registries to the same respective standards. So we're have been working with

ICANN Compliance, or sorry, excuse me, ICANN, since this trigger in December, and we've been working very well, closely aligned, we're working collaboratively.

And so although we can't necessarily share what those draft red lines are now, I just wanted to say, it's coming along very well. So we'll see more about those red lines, hopefully in the not too distant future. So these contract negotiations are not the end of this, this is something that we can do quickly, and then what we anticipate is that if there are other gaps, things needed down the road, that there can be other ICANN policy processes that can be done involving the entire community following the multi stakeholder model.

And the other thing to kind of keep in mind here is that this is not something we're doing to punish the good actors. There are registrars and registries, many of them in this room, who do take action against these types of complaints out there.

There's the DNS Abuse framework, which a number of registrars and registries here are signatories to. So we are doing things, but we don't anticipate that by creating these obligations, that it will come back and hurt us. And we're telling ICANN to make our contract stronger, and we don't want that to be something that has a result that's going to be negative for us. This is intended to go after those who are not feeling what we think are the obligations related to DNS Abuse. And this will help level the playing field so that all registrars and registries have to do this. That's it. Thanks.

REG LEVY: I don't see anyone in the queue, we probably have time for a few questions. Otherwise, we'll move on to the next agenda point and move along.

CHRIS DISSPAIN: Sorry, Reg, two things. There's a question in the chat, which if somebody can answer, it would be great. But also, am I dreaming, or does that say 7th of June 2024? And is that what we mean? I think we mean 2023.

REG LEVY: Is this why I was supposed to review this slide?

CHRIS DISSPAIN: Quite possibly. I just wanted to, before it gets picked up and runs. It's going to take them a whole year and a half. Does anyone want to tackle the question in the chat?

REG LEVY: I was actually in the midst of drafting it when Owen finished up. Yes, so I have addressed it in the chat, but if we if that comes up later, I'm happy to do so again.

OWEN SMIGELSKI: A second here. Apologies, I forgot about the second slide here. So this is the timeline where we are just showing what that is, not everything has dates, and as I see that the 2024 turn to 23 in there, so I'm

impressed, very efficient here. So those are what we've got coming on, and we don't necessarily have dates beyond where we are for step three. But the voting processes a unique and interesting, but we'll hopefully as we move ahead in this process, able to put more dates to those milestones that we have set forth there. Next slide. Pass this one.

BRIAN CIMBOLIC: Okay, then there's no questions here. We'll also have time for questions on everything at the end. If there's no particular questions on the amendment, then we will hand things over to Alan Woods and Ashley Hieneman, to talk about the CPH responses to the GNSO letters on DNS Abuse.

ALAN WOODS: Thank you very much. It's Alan Woods for the record. So yes, as people would have seen the GNSO chair sent letters to a number of different people within the community, including both the Registry Stakeholder Group and the Registrar Stakeholder Group, and there was two letters. The first letter was specifically relating to elements within the registry, accreditation agreement, sorry, the registrar accreditation agreement and the registry agreement, and one on the concept of what they were calling bulk registrations.

So we are putting in responses, but the first, I suppose the easiest one to deal with was a letter that we both put in a separate response to, and we can talk about that as on the one on bulk registrations. You'll see from the registry letter, it is an important thing to note that when

we are dealing with concepts that are being called bulk registrations, we're not very clear as to what that was indicating.

We talked about it within our own groups, and we came up with several different versions, several different definitions, and instead of going back and trying to muddy the waters, we thought it was best to go back and ask the GNSO to provide us with perhaps a little bit more specific detail before we could enter into it.

But that being said, we as a concept prefer the evidence-based escalation aspect, which if a bulk does occur, then the individualized elements of evidence that will be found from such an investigation would cover them all as far as we're concerned. However, that being said, we did point out that where the actual topic, and there's a distinct and well-scoped and defined issue to be reviewed and to be answered, then we are very, very open to having those conversations within the subgroups of both the registrars and the registries.

So from our point of view from the registries, and we thought it was pertinent to point at, for instance, the DGA work that we have done with the Public Safety Working Group has been one of those elements that it was a purely defined issue that we could work with, then we are very open on how quite successfully come up with a means by which we can address that. So as by way of giving an example of how we should do that, that was the point of our response on the bulk registrations. So with that, I can pass it over to Ashley.

ASHLEY HEINEMAN: Hello, this feels very far away. Excuse me. Yes, Ashley Heineman, Chair of the Registrar Stakeholder Group. And yes, we did submit our responses back to the chair of the GNSO today, and I've been informed they will be posted on a correspondence page. So if you're interested in reading these in detail, they will be ultimately posted for you to read.

But in respect to our response to the DNS Abuse, sorry, not DNS Abuse, the bulk registrations specific letter, it was very similar to another submission that was made by Graham Bunton, and that we have concerns with any particular focus on bulk registrations as a DNS Abuse items simply because it's not really a definable term, and possibly, not able to be defined either because there's legitimate ways in which bulk registrations are used.

What number are we talking, more than one, more than 100? It's just something that's really hard to come up with something that's going to be useful in the scope of DNS Abuse. For example, do you also want to be giving people a framework by which to work around our efforts? If you specify bulk registrations as a certain number, that's just going to lead people to allow up to that minus one number. So again, problematic in that respect.

When it came to the question of whether or not there should be work on this within ICANN or within our groups, we actually think it's not a good use of our time. There's lots of other areas that we can be much more effective in terms of focusing our efforts. So if it was up to us, actually, no, we would rather not spend time and resources on this

issue, and instead, direct them to someplace else that would be much more of a constructive area to work on.

So I'm trying to see what else is really impactful to say here so we can continue on into the conversation. But there is quite a bit more detail in our response. And we're thankful that this was raised and gave us the opportunity to respond and provide our perspective. But I think in terms of the grand scope of things, DNS Abuse has moved on, and bulk registrations, as people are characterizing them, really isn't what is a primary focal point for DNS Abuse, and that bad actors are using much more sophisticated ways to be bad.

So that's our response, and I encourage you all to read our responses, and happy to answer any further questions on that. And then I'll turn to the second letter that we received, which was more broadly focused on DNS Abuse and the recommendations that were made by the council small group. And we did a joint response to that, so you'll see just one letter from CPH. And basically, just want to thank the input that we did receive from the small team, it was clearly very well thought out and was very constructive.

And our response back is essentially saying that we hear what the small team has said, and we heard a lot of what other people were saying, and much of what was asked of us is now being addressed through the course of our negotiations on the contract. So more to come on that, but thank you to the small team, and those are our responses, and I encourage you to read them when you can. Thank you.

REG LEVY: Excellent. Thank you. Once again, I see no questions in the chat, so we'll go on to our next slide place.

BRIAN CIMBOLIC: Yes, and well, Alan can walk us through Privacy by Design, and PII Free Abuse Mitigation. Go ahead, Alan.

ALAN WOODS: Thank you very much. Alan, once again, for the record. So this was something that I need to slow down while speaking. This was something that I personally had gotten a bit of feedback from because identity digital, we put out an anti-abuse report now, and we're trying to do it on a quarterly basis to ensure a little bit more transparency in how we deal with abuse at the registry level. And one of the issues and the interesting tidbits that came up was a blog that we said, we actually don't use personal data in the registrant data in order to do our abuse management system.

We specifically, I suppose, a bit of hindsight, and the joys of being a European based was that seeing GDPR coming down the line, it was how could we evolve our means and our processes to remain effective in dealing with DNS Abuse at scale, but also being respectful of the expectations that will be found under legislation that would apply to a lot of our registrants, and to ourselves, of course, [00:18:41 - inaudible]?

So this is the concept of that many of us will be very familiar with, and that's the Privacy by Design concept that's within the general data

protection regulation. So the blog is LinkedIn, and you can see the slides and be able to link to the blog, It's a very small blog, but it is pointing out that we have taken a stand in the sense of we do not believe at the registry level, that the use of personal data that would be traditionally present in the registrant data is of use in our abuse management expectations from that of a registry operator.

In the past, and this actually kind of leads a little bit into the concept of the bulk registration. It's very hard at the registry level, at this point, to use registrar and data as a correlation the personal data and registrant. So we took the stand and said, no, we're just not going to use it in the system that we use in our back end system.

There's a little point at the end here, it's important to note that, yes, the correlation of registering data may be useful, but it may be useful farther upstream or downstream, depending on your point of view in the abuse management process. We don't have enough of that data to be able to make strong conclusions that would not end up being arbitrary and its conclusion of like for like, or, as the lawyers in the audience would understand the similar fact evidence of it all.

So that was that particular decision and why we took that decision to just remove it, if it was of no necessity to us in our process. Next slide, please. And just to dig down into the concept of necessity, and this is why we came to that decision. But we felt that we had no legal basis to actually use this registrant data in order to achieve something that we have achieved and continue to achieve, we hope in a very good and continually high-quality way, without using this data. Therefore,

having it just because is probably not something that we needed in a third-party system, and within our own systems for that purpose.

And again, that's going to the very core of the concept of privacy by design, and, indeed, privacy by default. We, and I mentioned this as well earlier, we now just escalate based on clear expectations of an evidence-based threshold, if there is evidence of an abuse, we will escalate that abuse, it doesn't matter who registered it, the evidence is there, and it speaks for itself. We will escalate that to the registrar and the usual course of things, and they can deal obviously, and they should more likely deal with the registrant in that instance if they see fit, and if they believe that that is the right thing to do at that point.

So there's a few statements here, but I think the important one is we simply cannot justify data processing where we don't have a tangible benefit to show for it at the end of the day when it comes to personal data. And that really is the core of proportionality when it comes to the use of that data. And you can see something else that we put into our blog as well was we have done an overview of the data that we hold in our registry, and 70%, it was over 70% of the data that we hold, actually doesn't contain registrant personal data anymore.

So we're still looking at 30%. So in hindsight, we were very happy that we took this step and we tried to evolve beyond the use. And we believe that we're doing it as well as we can do at the moment and quite effectively, given, you can see from the reports itself. So why we're bringing this up at the moment is just to have that conversation, to give an idea to the community into how we are evolving given the GDPR and its similar legislative enactments throughout the world that

are cropping up, and that it is possible. It's possible from the registry point of view, and we are happy to share our results on that as time goes by.

BRIAN CIMBOLIC: Thank you very much, Alan. Any questions for Alan? Okay. Great stuff, Alan. I would also note identity digital isn't alone here, we too at PII are focused on evidence based reporting, and it's led to really higher quality reports that have become more actionable when we send it downstream to the registrars. So thanks, Alan. Good stuff. Next, I'm going to hand it over to my co-chair Reg to talk about acid tool. Reg.

REG LEVY: Thank you very much. Next slide, please. So ACIDTool.com is a service provided by the Registrar Stakeholder Group that allows people to perform a Digg lookup in an easy format, and get information on a domain name. This is useful when somebody is doing something bad on the internet and you don't like it and you would like to find out who to complain to. It provides you with a hosting provider. So if that information is content that you would like to complain about, that is a good place to start.

It also provides the email service provider so that if there is an email issue, spam that does not rise to the level of DNS Abuse, you can contact the email provider. It includes the full WHOIS output, including creation date, and reseller name, if applicable. And it includes the registrant data if in fact, the registrant has opted into

publishing that. It also includes the registrar contact information as part of the standard WHOIS output.

But we're hoping that this will be useful for people so that they can figure out who to go to before escalating directly to the registrar, or even further to the registry when there's something going on that doesn't actually fall under DNS Abuse. So it stands for Abuse Contact Identifier because these are the abuse contexts for hosting providers and email server As providers. Again, not DNS abuse contact. So please feel free to continue to send that stuff to the registrar.

Next slide, please. Very briefly go to ACIDTool.com. Because of a flood yesterday, some other domains might redirect into the ACIDTool.com. Put the domain name into the domain name field, and hit enter. And you should get back the data that you are looking for and data that will help you find the right parties to contact, then you can proceed, of course, to contacting them directly.

Next slide, please. So we've been tracking some statistics since we premiered ACIDTool.com in September of last year. And we saw a spike in unique visits, obviously, as soon as we premiered it. But we've seen it sort of tapered off to a reasonable number that we see growing slightly but steadily.

So we hope that this means that it's becoming useful to more and more people. In addition, it has about the same number of hits monthly. So even though we've seen a decrease in unique hits, we've seen the same number, excuse me, decrease in the number of unique visits, I've seen a steady number of usage hits, which means that the same people who are coming to the site are using it multiple times.

So again, we think that this means that it is in fact useful. We've heard from a number of different parties that they are using it, that they are distributing it, so we're very hopeful that this is a tool that can be popularized throughout the broader internet. And I'm going to turn it back to Brian now. Sorry, questions, I guess.

BRIAN CIMBOLIC: Thank you, Reg. Do we have any questions? No questions on ACID Tools. Okay, next slide. And next slide, please. I'm going to hand it over to Owen, I believe to talk about some work on AGP limits. Owen, take it away.

OWEN SMIGELSKI: Thank you, Brian. So this is something that has come out of the Registrar Stakeholder Group, excuse me, Abuse Working Group, and we've just started to collaborate recently with the registries on this, and it is another potential way to help combat DNS abuse. So for those of you who are not familiar with one of the ICANN's now less used consensus policies, it's the AGP limits policy, and the AGP stands for Add Grace Period. And that is the first five days within the creation of a domain name.

And when this was created, because at one point, what would happen is 1a domain name would be registered, somebody would check to see how much traffic went to it. And if it was a lot of traffic, they keep it, if it wasn't a lot of traffic, then they would just get rid of it. And what this led to was a lot of domain names being deleted. And I think if I recall, some of the estimates were that up to 90% of domain names being

registered were then being deleted each month. So ICANN, obviously, the community needs to do something about that.

And so in 2009, the AGP limits policy was established, and this was to combat what was called domain tasting, and that was what I was referring to earlier. And so the AGP limits policy gives a cap to the number of domain names that a registrar may delete per calendar month. If the registrar exceeds those limits, then a registry cannot refund or give rebates basically or refunds for deleting domain names back to that registrar, because if you delete it within that period, then you don't have to pay the registry for it.

And the thresholds for this is 10% of new registrations or 10% of registrations per month, or 50 domain names, whichever is higher. At the same time that the AGP limits policy came into place, ICANN also added the non-refundable 18 cent fee per domain name. And those two in combination essentially ended domain tasting. That's not really a problem, and it's something that we don't really talk about too much because it was solved. The problem is that was back in 2009, it had been a problem for a while, registrars are now a little bit more savvy in detecting abusive and or fraudulent domain registrations within that period.

What we see is quite often somebody will register a domain name either using a hacked PayPal account or stolen credit card or a generated credit card, and we will know within days of that have notified by the payment processor about that fraud. And using the word abusive and fraudulent, I just want to make sure that those are

two separate things. Abusive means DNS Abuse, and the other one is fraud or somebody's conducting fraud with the payment there.

So when this happens, a registrar needs to keep the stolen money, so they have to refund the money to the processor, and then also the domain name gets deleted. What we're finding is that these deletions because of sometime-- and quite often what we found is, and surprisingly, people who are registering domain names for bad purposes are using it with stolen money or illegal means. So we do need to take action against these, these are things that could either are actively being used for or likely could be used for DNS Abuse. So they need to be deleted, but what's happening is registrar's are exceeding those limits.

So then they don't qualify for a refund. There is an exemption in the AGP limits policy, but it's under extraordinary circumstances. So it's not interpreted as something that could be ongoing or continual, or as we've seen it Namecheap, a campaign of six months of a ridiculous amount of domain names being registered for a campaign, that then the registrar asking for a refund the money to the payment provider, and then maybe make the decision of just not deleting the domain name to still qualify for a rebate.

So it's a big financial hit. So what we're doing is drafting a proposal that would ensure that registrars can action DNS Abuse and payment fraud without incurring these additional financial penalties. We want to make it a financial incentive for registrars to take quick action when abuse of domain names are being registered, or when payment fraud is involved with that. So we're still working on this proposal, it's not

ready for public discussion yet, but hopefully, we'll get to that point soon. So I'll pause if anybody has any questions.

BRIAN CIMBOLIC: Thank you. Well, when we actually do have a question. Farzaneh.

FARZANEH BADIEL: Hi, my name is Farzaneh Badiel, commercial stakeholder group. Sorry, the design of this room is just not for outreach. So I just wanted to ask the word fraudulent makes me nervous, what do you mean by fraudulent and how that has been defined?

OWEN SMIGELSKI: So I'm just using a shorthand here, but what I'm referring to is when we see this, often it is through, somebody loses access to their PayPal account, meaning somebody hacked it, stole it, is using it, or somebody's credit card number has been stolen, or they're using a credit card generator to come up with names.

So these are all completely illegal types of payments, criminal activity. I would probably perhaps come for a better wording in there if that's a concern, but it's people who are-- monies being stolen from people whose it's not theirs is how that's working out.

BRIAN CIMBOLIC: Thank you, Farzaneh. We also have a question if okay, going back to Alan, we have a question from Sara Wilde in the chat. She says, "I

understand that you use a provider for DNS abuse management, can you tell us more about who that is?"

ALAN WOODS: Thank you very much. Alan Woods for the record. Thank you, Sara. And of course, I completely missed it when I was talking. It is a company called Clean DNS that we use. They've worked very closely with us in realizing the dream of a PII free abuse management in order to get across. So Clean DNS is the company. So thank you so much. I'm sorry that I didn't say it in my presentation.

BRIAN CIMBOLIC: Thank you, Alan. And Sara, sorry, if I missed your question previously. Does anyone have any other questions for Owen or back to Alan? Okay, if not, then we can hand things over to Graeme Bunton and Rowena Schoo, to talk about some-- Oh, sorry, we do have a follow up. If we could go back to the AGP limit slide. Sorry. Farzaneh, go ahead.

FARZANEH BADIEL: Sorry, I just didn't know that we are going to move to the NSA. So I'm going to ask this question that is general, I'm not presupposing anything. When we were in discussion about WHOIS and privacy and before coming up with EPDP, there were these rumors that the contracted parties are going to have these bilateral negotiations with ICANN and they are not going to allow the community to do the multistakeholder process, and every time they are kind of like, but I disagreed with that, it's in our bylaws, and they can't do that.

So then this brings me to the question of, so which provisions of the bylaws did you use in order to start these bilateral negotiations? And with this, how can we ensure that this does not, I'm not against it, I'm just saying how can we ensure that this does not set a precedent for later on when we want to actually work on issues with multistakeholder man, if that's a good idea, even?

OWEN SMIGELSKI: So, the registrars and registries are not necessarily bound by the ICANN bylaws, we're bound by the contracts that we signed with ICANN, which were created through the the multistakeholder model. I know the base RA and things like that did go through those reviews, the 2013 RAA also went through a process of community involvement. A lot of this also predates when a bunch of us were involved with ICANN.

So the most recent revisions of the RA and RAA included a section specifically in there how negotiations could be triggered by ICANN-- or closer. Okay, I'm sorry. I didn't realize how close I have to get to this microphone. And slower, apologies. I'm all flustered.

Yes. So those are in there for ICANN to initiate those. And similar to what happened during the RDAP amendment process, the initial discussions go on between ICANN and the contracted parties. That's not to say that the rest of the community does not get involved, but it's at a point when ICANN and the registrars and registries have established something which we think works.

And then that does go out for public comment, and as with what happened during the RDAP negotiations, we review the public comment, and if it's necessary, we do make tweaks, changes, modifications, or provide an explanation as to why that may be out of scope or not applicable to that.

BRIAN CIMBOLIC: Thank you, Owen. And thank you Farzaneh, and you kind of got the queue going here. So now we actually-- I think Catherine Merdinger wants to respond, and then we have Greg Dibiase, and Mark Datysgeld with questions in the queue as well. Go ahead, Catherine.

CATHERIN MERDINGER: Thank you. I just wanted to jump in to say, this is not the first time these contracts have been amended. If there was an argument at that time, I wasn't here, but we're not allowed to negotiate our contracts with ICANN, I would be interested to hear how that went last time. But if it's more about the subject matter of these negotiations, there is a plan to have community input both in a public comment period, and we also think this sets us up better for more conversations with the community and more work on how to address DNS Abuse, and the methods with which we do that.

So we're not trying to be shady, and all that kind of stuff, but this is how the contract amendment process has always worked. And I don't think it's fair to import some kind of nefarious, anything, which I don't think is what you did, but I just want to be clear, we're doing exactly what we've always done.

BRIAN CIMBOLIC: Thank you very much, Catherine. Okay, we have Greg Dibiase in the queue, and then queue building. Go ahead, Greg.

GREG DIBIASE: Yes, this is Greg Dibiase for the record. So I just want to add to the point on kind of the multi stakeholder nature, I guess, genesis of this work. So this at least partly stems from work from the DNS Abuse small team within Council, which contains all the constituencies across the GNSO. This wasn't a specific registrars and registries going in their own room and doing something, this was a group composed of all SGs that took input from across the community. We asked input from Compliance, ALAC, GAC, and the letter from Compliance identified that there may be this part of the contract that is ambiguous.

So that was at least part of the impetus of where this is coming from in the first place. But I think that's important context when we're looking at this negotiation. Yes, in this phase, it is between contracted parties and ICANN because it's to contract between contracted parties and ICANN. But the genesis of this, I guess I would say it's fair to say has its roots in the multi stakeholder process.

BRIAN CIMBOLIC: Thank you very much, Greg. And big plus one to that, the letter that the CPH sent to sort of kick this process off, directly decided to the work of the GNSO small team and it was largely in response to that. So

we have Mark Datysgeld and John McCabe, and then we're actually going to draw a line in the queue for now. There will be time for questions in the end, but we want to make sure that we're able to cover all the material, and then take questions at the end. So Mark, please go ahead.

MARK DATYSGELD: Now it's on. Sorry, let me-- there we go. So Mark Datysgeld speaking, GNSO Council, co-chair of the small team on DNS Abuse, Just a quick shout out to the CPH, it was really good to get a prompt response from you. And this was a process that was interesting because we started from reaching out to the entire community, we got input from pretty much every ICANN stakeholder and build on top of that, we were able to communicate directly with you, you gave us a very thorough answer. And this is pointing towards one of the many ways we can do work in ICANN, and I feel that it has been a very healthy relationship, I hope you felt respected by our team during this process, and we felt that respect back.

So moving forward, we'll take all of these answers back to the Council in our next meeting, we'll go through them, we hear on bulk registration, and we'll see if that is a priority and whether it fits. And we definitely look forward to the process of negotiation and keeping in mind that the community is very interested in providing public comments, it's very good that you're addressing this matter, because we have heard loud and clear from the community that this is a priority, and we as the council would like to see that as a priority.

So thank you very much for the work so far, that's doing good work. At the end of the day, this is about rooting out the bad actors who are not us. So thank you very much, everyone, and let's keep working.

BRIAN CIMBOLIC: Thanks so much Mark. And just a kudos to the GNSO DNS Abuse small team and the work that the GNSO largely has been doing on this. So thank you very much for that. John McCabe, and then we will hand things over to the DNS abuse Institute. John, go ahead.

JOHN MCCABE: Thank you. I'm over here. I just wanted to say that I think that we're talking about DNS Abuse, and it's interesting that this subject that Owen has raised is coming up, because I think from the beginning before there was ICANN, and that still today, it is called a sponsoring registrar. And that indicates to most people that they are the sponsor is like bringing this person into the community. And so, when you end up in a situation where there's a business issue, which is accepting payment from a customer, and then it turns out to be fraudulent, I think it means that well, who was the customer to begin with?

It seems like that is a real channel for DNS Abuse, it's not knowing who you're dealing with, who the registrant is. And that's what I'm hearing here is, there should be this giveback of by ICANN of the fee, when in fact, it's somebody you don't know could be put on 30 days wait before they get their domains activated, or 60 days, or whatever it has to be, that's a business decision. But I think it's to do a good back of

the AGP feed is ICANN subsidizing domain abuse. That's my comment. Thank you.

BRIAN CIMBOLIC: Thank you very much for that, John. Okay, we have one response from Crystal, and then we are going to draw a line and move on to the institute uptake. Crystal, go ahead.

CRYSTAL ONDO: Yes, I just wanted to clarify, we're not talking about asking ICANN for the feedback, we're talking about the registry refund that happens in the first five days when you delete it. So just a point of clarification there.

BRIAN CIMBOLIC: Thank you very much, Crystal. Okay, Graeme Bunton and Rowena Schoo, we are going to hand things over to you.

GRAEME BUNTON: Thank you, Brian. Hello, everyone. Good to see you. My name is Graeme Bunton. I'm the Executive Director of the DNS Abuse Institute. Next slide, please. We've got a fair amount of content to get through. I'm going to try and do my NetBeacon update really quickly because I think Rowena has got some really interesting stuff to show from our campus initiative, and I want to make sure that we leave room for questions. So we're around all week. Please feel to reach out if you've got questions that we don't have time to get to here.

Next slide, please. So NetBeacon for those who are unfamiliar is the centralized abuse reporting system that the DNS Abuse Institute created and launched last year. It is a direct response in many ways to a number of different ICANN outputs, SEC 115 is the most obvious of those kindly developed by Clean DNS, where they adapted some of their technology and donated a bunch of development time to adapt it for our purposes.

It's a free service, anyone can use it, and it solves the problem of how do you report abuse because there's a one stop shop to go to where you can just go to the website, anyone can use it, relatively easy to use forms to submit abuse reports to all ICANN accredited registrars. And it's free for registrars to use as well so that they can get clean, well formatted, easy to parse abuse reports that are enriched where they want them.

Next slide, please. So we've talked about this, I think we launched it just ahead of the meeting in The Hague last year, and we talked a little bit about it and KL as well. So this is just my brief update on where we are and where we're going. Deliverability has so far remained really high. We do still occasionally discover a registrar who is auto responding to a form, and so we do some outreach in those circumstances. Usage has been enjoyably steadily increasing, we expect that to be pretty high by the end of this year, and that's my sort of key corporate goal. So if you haven't talked to me about this yet, and you're interested, you're going to hear from me.

We've recently opened the submission API so that people within the community or outside, internet security experts can connect to

NetBeacon and report abuse at scale, and so that's pretty fun. We're looking at pushing some of the data that we get into our compass initiative, which we'll talk about in a minute, into NetBeacon. And this is going to operate as a shortcut to a industry specific abuse feed so that we're now pushing through evidenced high quality abuse reports to the entire industry. And so I'm very excited about the potential there.

One of the things that happened as we're building this and sort of specking it out was I spent 10 years as a registrar, and so it very much was built with me thinking about registrar problems, sort of unsurprisingly. And so I think we're now in a good place where it serves registrar needs pretty well. There's more to do there, of course, there always will be, but that side of the equation is good. On the other side, what are the features that abuse reporters need in order to be successful in using NetBeacon.

And so now we're turning our attention to that space, making sure that the people who have abuse reports and need to get it somewhere, have the pieces in place with NetBeacon that's going to make that experience great. And so working on that, the most recent feature is that we've enabled abuse reporter verification.

And so if you are a representative of an organization that has abuse to report, you can request by an NetBeacon to be verified, that's really do we recognize your organization, or can we find something about that organization, and do you control an email address from it? And so it's a manual process that Rowena and I do. And that gives you access to a couple of new features where you can make sure that you're including

who your organization is in the reports that you submit through NetBeacon, as well as include boilerplate text on every report that you submit.

And so that just makes it a little bit clearer when you're using this as your channels for distributing reports. Who you are, what your expectations might be, how to contact you, things like that. Always happy for more feedback. We're always trying to make this tool better. Again, it's a free service for everybody. If you're interested, please come talk to us to learn more.

Next slide should be a screenshot of just how you can add your organization name to the referrer. Most registrars are getting reports via email, some by API, but that's what that would look like in the settings.

Next slide, please. So couple things that we're planning on, working on, report receipts so that if you're submitting via the UI, like the actual website, as opposed to API, you can choose to get an email receipt, report monitoring so that we can follow what's happened with those domain names over time, which is a little bit funny because attribution for mitigation can be difficult, and mitigation, like turning the domain off might not be the right answer every time, but we're working on doing that.

We will be integrating a number of ccTLDs this year. We'll also be expanding the list of harms as well as the list of recipients. And so there's lots of work to do, there's a hilarious number of really fun problems to solve, but I think the future for this service is pretty bright. So please check it out if you haven't. And I think that's it on

NetBeacon. And I'm going to hold questions to the end, because I think what Rowena has got coming is the really interesting stuff, and so I'll pass it over to her.

ROWENA SCHOO: Thanks, Graeme. Next slide, please. It's Rowena Schoo here, director of programs and policy at the DNS Abuse Institute. I'm going to talk to you a bit about our other project, which is called DNS AI Compass. If I could get the next slide. So we launched Compass in September last year, and this is our project aimed at measuring phishing and malware. So we look at the prevalence, the persistence, whether those issues are being mitigated, and also the registration type, whether it's compromised and malicious. So since September, we've been publishing data monthly, and all of this is a high level aggregate data. So that's out there in the public domain.

Now, you can look at it at that link on the slide, and I've also dropped it in the chat as well. Next slide, please. So in terms of where do we go from here, there are two directions that we're working towards. So the first is around closing that gap between the data that we have, which is quite substantial and broken down into individual TLDs and registrars, and what we've put out in the public domain, which is high level, generalized information.

So there's two things we want to do. One is around publishing some metrics in a more granular way, publicly. So this would be identifying individual registrars and TLDs who are consistently performing well, or ones that are in need of a bit of improvement. I'll talk a little bit more on the next slide about what that might look like.

The second thing that we're looking at-- sorry, could you get back a slide. The second thing that we're looking at is these individualized dashboards for registries and registrars, and those are even more detailed, these are not something that we were initially thinking that we would ever publish. They are really for the individual operators to understand more details about abuse in their area of responsibility, and to understand that over time, and compare that to their peers.

Okay, next slide now. So, on the metrics for public reporting, we're intentionally doing this very carefully, and trying to be very, very thoughtful about what we put out into the public domain. The reason for publishing it initially is to improve industry performance by focusing effort, and also to encourage data driven policy decisions as these discussions are ongoing in the community. We are conscious that the metrics we put out should target specific behaviors by registries and registrars, where we think those behaviors can be changed to make a difference, a positive difference on the abuse landscape.

And as a result of that, we're really, really conscious that there could be unintended consequences, or over corrections based on what we put out. So we're being very careful about how we do that, and we're spending a lot of time engaging with the wider community. And I really, really encourage anyone who's here today to reach out to us to have a conversation about this.

We want to understand what information the community would find useful around DNS abuse, and we want to hear from a broad range of people around what makes sense, what information is helpful, what

might be the unintended consequences of certain information being out publicly? So we're thinking very carefully about that.

We're still progressing towards publishing that information, hopefully, very soon. We're also operating in a sense of having no surprises as much as we can help it. So if there are registries and registrars who will be named in that reporting, we will do our best efforts to contact them and reach out to them before that. So yes, that's the public reporting.

If you could go to the next slide. So the second piece, I mentioned the individual dashboards. So the reason for creating these is really to empower registries and registrars with that data. And what we're finding is as we discussed this with people, a lot of people are saying this is incredibly helpful for them to see while they're making changes or trying to do things internally to address abuse. And what we want is to provide them with a consistent metric and something that's objective that they can use to compare over time, and something that they can use to get a sense of where they're doing in relation to their peers and the wider landscape.

The reason for showing you what we're going to show you today is both to encourage registries and registrars to come and have a chat with us and view their own data. So a bit of awareness raising, but it's also to encourage that wider dialogue with the whole community about what information is useful and what you'd like to see. You should get a sense from this quick whistlestop tour that I'm about to show you about the type of data that we have and the ways that we can present that. And I'm just going to note this is a work in progress.

This is a look under the hood, the type of data that we have, as we build these dashboards, and extend a really big thank you for the registries and registrars who have agreed to let us share their data with you here today.

So the DNS Abuse Institute was of course created by Public Interest Registry. So we naturally asked PIR for permission to show you the .org data. We also have an advisory council at the institute. And on the advisory council, we have representatives from Google registrar and GoDaddy, who have both also kindly agreed to let us show you some of their data here today. So thank you to those people who are helping us there.

Okay, next slide. Okay, so I'm not expecting you to be able to read every detail of that. The point of showing you this is to give you a sense of how where we're thinking about the data. To this dashboard, the top is Google, and the bottom is GoDaddy. The stats down the left-hand side are giving a sense of how many domains we see under management, how many newly registered domains there are, how many unique domains were identified as phishing or malware, as observed by a methodology, how much of that observed abuse exists per 100k of DU. So we're trying to get a sense for scaling abuse with the vastly different size registrars.

And then the third sort of box there is around the percentage of new registrations that are observed as being phishing and malware. To the right of that we're including some concepts around the range in those three metrics, the median as data tends not to be evenly distributed, so we're using a median rather than an average. And then we've also

got some concepts around a peer group. It's incredibly difficult to group anyone into a peer group in this industry. At the moment, we have just gone for domains under management that's purely based on size. So both GoDaddy and Google are currently in the largest tier, which is over 3 million. Don't worry too much about zooming.

Okay. Then the final metrics on the other side of this chart is around proportionality. So if we expect that abuse is evenly distributed across the ecosystem, then we would anticipate seeing that the proportion of abuse that any registrar has, it correlates to the proportion of the domain names that they hold. What we tend to find as we're looking at this data, is that abuse is not evenly distributed across the ecosystem. You won't probably be able to read the stats there, but both of these two registrars appear to be under indexing on the abuse they hold compared to the domains that they hold.

Next slide. So we also have some more detailed charts available for registrars to see, and this is where we compare their observed abused to their peers. So that's the chart on the left here. We've, of course, redacted the other registrar names that are listed below that. The chart on the right is in the same order, but it's abuse per 100,000 domains under management. And you can see that the relationship between abuse and size is not particularly clear.

Next slide, please. This is the same dashboard cut for GoDaddy. We've also got below that a chart that is looking at that comparison between the proportionality. And then there's also a chart on median mitigation time. We have redacted this essentially out of an abundance of caution for putting anything out into the public domain

that could be weaponized by someone with malicious intent. Because what we're finding as we go through this is that we're quite sure that these mitigation times reflect the internal policies and processes that a registrar uses to tackle abuse.

So we've been quite cautious about not putting anything out that would say, okay, I get X amount of time at X registrar, I can utilize that to my advantage. But I should actually note that some registrar's have incredibly low medium mitigation times. And GoDaddy is actually one of those, so is Namecheap.

Next slide. Sorry, I'm being told to hurry up, which I should do. The binary dots in here are around giving a registrar their view into their data over time. So how much phishing, how much malware, and how much is being mitigated. We also look at how much is compromised and how much is malicious. So there's fishing on the left, malware on the right, compromised is pink, malicious is purple. If you can go to the next slide. We certainly noticed that different registrars and different registries have different breakdowns of compromised and malicious, and that tends to reflect the age, the type of customers, larger, older registrars and registries tend to have more compromised domains.

Next slide, please. And again, there's some more things on mitigation. Next slide. And then this is the registry dashboard. So same data, but presented for the registry. PIR also appears to be under indexing compared to their size.

Next slide. And then this is the same version for registries where we're looking at their observed abuse, breaking that down by per 100k,

looking at how much is compromised, and how much is malicious, and their mitigation compared to their peers.

Next slide. And what you'll see here is overall phishing and malware on the left, a mitigation rate on the right, should just be aware that these are the charts I've been showing you on mitigation include both compromised and malicious. And again, we're seeing that trend in the older registries, they appear to be more likely usually to have more compromised domains, which seems to make sense because they have more domains that have been around for a long time and have had that time to become compromised.

Okay, I think that's the last slide. So the take home message, come and chat to us. I'll put a link in the Zoom chat around how to book some time with us, and even if you want to chat to us post ICANN, we're always happy to do a virtual call. We'd really love to hear your feedback. Graeme, you want to add anything, or do we have any questions in the queue?

GRAEME BUNTON: We do have questions in the queue. So I think we have Steve, and then Farzaneh. Steve.

STEVE DELBIANCO: Thanks, Graeme. Steve DelBianco with the Business Constituency. Very good presentation on both elements, but I wanted to see how they tie together. To the extent that you have granular data about the quality and length of time it takes to mitigate, do you think that the

vocabulary of the data you capture is going to match what the obligations will be in the revised RAA and Registry Agreement?

In other words, the first half of today's briefing was about pending contract obligations changes, and very precise language is important. So with respect to an obligation to mitigate, which may or may not emerge from the contract negotiations, will Compliance be able to rely on Compass drill downs to find corresponding instances where registrars are not meeting the new obligations? Do you think it'll be that granular, and will the definitions and words be that consistent? Thank you.

GRAEME BUNTON: Thanks, Steve. I don't know that I can comment on what's happening in the negotiation, so I'm just going to put that aside. Re-data for Compliance is an interesting discussion. I'd have to think about how they would use that and what data would be useful for that. Mitigation is a funny thing. Generally, we see from this data that the rates are generally really quite high. We were very pleasantly surprised as we were building up this project to see just how much mitigation happens.

I think we need to get more sophisticated in our data to understand better the distributions between how mitigation happens between compromised and malicious, because there are many circumstances where mitigating for a compromised domain name is not the right solution, like taking it offline is not the right solution. And until we can really disambiguate those circumstances, I don't think it would be

appropriate to really rely on this sort of data for that sort of situation. Thanks.

BRIAN CIMBOLIC: Thank you, Graeme. Thank you, Steve. We have Farzaneh, and then Owen.

FARZANEH BADIEL: Yes, Farzana Badiel of Non-commercial Stakeholder Group. So I have a question to grab on your slide. You had plans to expand the list of harms, what does that mean?

GRAEME BUNTON: It means that there's lots of bad things on the internet that need to get to the places where the people can deal with them. And bifurcating abuse reporting processes introduces complexity that I think we might have some opportunities to solve. There's no intention here to obligate anyone to do anything, because of course, we can't do that. But you're right, it's an interesting question that requires more engagement. And so as we begin to do that, let's talk some more about it.

FARZANEH BADIEL: Can I do a follow up? So what do you mean, like on the internet? Like, are we tackling every harm that is happening on the internet? So this is like limited to DNS Abuse, but is it like, limited to technical? Because

harm is the consequence of abuse, so just tell me a little bit how you define that.

GRAEME BUNTON: I suspect that this is a much longer conversation, so let's try and take that offline. Thank you.

BRIAN CIMBOLIC: Thank you, Graeme. We have Owen, and then we have Crystal.

OWEN SMIGELSKI: Thanks, Brian. I was going to give a comment to Graeme about just something Steve was raising about whether the DNS Abuse negotiations will have an impact on mitigation. A lot of the registrars, registries that are involved in this process are in the stakeholder group are already mitigating this, and so I would expect that our times would change that much. It would be for the others who are not necessarily doing that, the ones that have the higher levels of abuse, the ones that let the abuse sit forever, although we would expect to move the needle on that, but that's to be seen.

I just would like to put a plug in for a NetBeacon and the abuse reports that come in there. I know it's complicated for those of you out there who file abuse complaints, you have to find the registrar, you have to do this, you have to do that, whatever, NetBeacon is great. It's in one place, it does it all for you, and on the plus side, for a registrar, when we get a complaint from NetBeacon, it's got the evidence, it's got the stuff in there, they've run some checks, it makes it a lot easier for our

team to review, we get abuse complaints sometimes that include 20, 30-page letters that our team just doesn't really have the bandwidth to deal with. So we really appreciate NetBeacon, and encourage everyone to use it. Thank you.

BRIAN CIMBOLIC: Thanks, Owen. Crystal, and then Michael, and James. Crystal.

CRYSTAL ONDO: Thanks, Crystal Ondo, Google. I think Steve, you might be also completing, this as a separate effort, not by Compliance. So this data, right is not something that would be relied upon by Compliance, OCTO is in the room, they also track data to some extent and in the same manner.

I think one thing that is useful and one reason why we're very engaged with the DNS AI is because registrars track their own data, but the data you see does not often match the data that is seen publicly. We've seen lots of published reports of this data versus that data. So it's another interesting point for registrars to take into consideration when they're looking at their abuse. Go to Graeme and Rowena, look at what they're finding publicly, and if it doesn't match your data, figure out where the disconnect is.

I think it's a really important tool for registrars and registries to use in that manner. It's very informative, and the trend over time helps me go back to my team and say, okay, we've seen this externally, why is

that and dig into it. So it's not necessarily to hold us to account, but to improve the processes we already have in place.

BRIAN CIMBOLIC: Steve [01:08:54 - inaudible] you mentioned, go ahead.

STEVE DELBIANCO: If I could follow up. Thank you, Crystal. No confusion here, I understand the completely the different efforts, but understanding also that if the contract amendments make more significant obligations for the quality and time of mitigation, then the bad actors were never in the room with us anyway, will could be potentially more easily identified by a drill down on the DNS Abuse Institute Compass recording and drill down at the registrar level.

That would clearly not be enough to find a registrar in breach of contract, it would simply be the starting point for observing the compliance audit put some attention onto these four registrars as Graeme has given us the data to show that they're trending in not a good way and their numbers are becoming significant, and that just begins the process. And I had phrased my question out of hopes that the contract amendments would have the same vocabulary that is in the report so that the word mitigation might mean the same thing, and that DNS Abuse would mean the same thing in Graeme's reporting, as it does in the contract amendments. So I'm sorry, I didn't make that clear.

CRYSTAL ONDO: Yes, and just to say, I think we're all violently in agreement with that.

BRIAN CIMBOLIC: Thank you, guys. We only have four minutes left, so I'm going to ask you guys to keep it relatively brief. We have Michael, then James. Michael.

UNKNOWN SPEAKER: Just lost him [01:10:22 - inaudible], not in the Zoom.

JOHN MCCABE: Thank you, John McCabe. I just wanted to-- Graeme, one last time, we were in the same time together, we had an exchange, and I put forth the proposition that the registrars could use pending create status when they're dealing with a customer that they don't know who's paying by credit card, and they order on a Friday night, they can make those value judgments, but some unknown quantity that comes in and might cancel it.

But Mike might have the card fail on it before days and still be eligible for AGP rebate, but I'm wondering, you said you would look into that as a possibility. I was wondering if you had had any chance to discuss that or investigate it, and what your feedback was?

GRAEME BUNTON: I'm sorry, John. I don't recall the specifics of that conversation, so we'll have to circle back on that again.

JOHN MCCABE: Okay, thanks.

BRIAN CIMBOLIC: Thanks, Graeme. James.

JAMES BLADEL: Hey, thanks, Brian. Graeme, Rowena, thank you, great tool, really appreciate the work you've done here, and I am also grateful for you including us in the trial run of some of the dashboards. I think like Crystal, it's going to be a very valuable tool for us.

But I want to circle back to Farzaneh's question, please, because as you're talking about the evolution of this tool going forward, and she's, I think very astutely picked up on the idea that when you talk about expanding categories of abuse, can we just be clear that the institute will stick within the established definition of DNS Abuse as it is discussed within ICANN, as it was discussed within the framework documents, and not necessarily go out and beyond those five categories of abuse?

GRAEME BUNTON: So there's a lot of complication here, and I want to make sure that we're not taking time from other stuff. Compass measures only DNS Abuse, will only ever touch DNS Abuse. NetBeacon as an abuse reporting intermediary while we were developing those requirements, looked at the reporting, the abuse reporting webpages for the top 50

or 60 registrars, many of them accept abuse reports for things other than DNS abuse.

So it could be a DMCA notice for American registrar. If they're trying to accept reports for all of the abuses that they do, to ask them to go, customers, people reporting abuse, to go here for these categories that they probably don't understand, and over here for this other category of abuse, presented basically a user interface problem.

So figuring out a way that we could accept abuse reports for a registrar for everything they choose to accept, so that we can have registrars opt in to go oh, yes, we also want these to other types of harms, so that they can concentrate all of that reporting into a single place, is the features that we're looking at. Does that help you?

JAMES BLADEL: It helps, but just I would encourage you to engage with especially the different peers that you've already engaged with, if you expand beyond -- DNS Abuse Institute, it's in the name, let's stick to that playground.

GRAEME BUNTON: Just to be super clear, there's opt in, not presented, so it's available as features for the people who choose to engage with them.

BRIAN CIMBOLIC: Okay. With that, there's one minute left. Any last? Okay, well then, thank you very much, everyone, another productive session. Thank you for coming and participating.

SUE SCHULER: And we can end the recording.

[END OF TRANSCRIPTION]