ICANN75 | AGM – GNSO: BC Membership Meeting
Sunday, September 18, 2022 – 15:00 to 16:00 KUL

BRENDA BREWER: Good morning, good afternoon, and good evening. I'm Brenda Brewer. Welcome to the Business Constituency Membership meeting at ICANN75. 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 be read aloud if put in the proper form as noted in the chat. If you would like to ask a question or make a comment 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.

This session includes automated real-time transcription. Please note this 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 multistakeholder model, we ask that you sign in to Zoom sessions using your full name. For example, first name, last name or surname. You may be removed from the session if you do not sign in using your full name. And with that, I will turn the floor over to chair Mason Cole. Thank you.

MASON COLE: Thank you very much, Brenda. Everybody, please wish Brenda a happy birthday. All right.

BRENDA BREWER: Thank you.

MASON COLE: Happy birthday, Brenda. We do need a cake. All right, ladies and gentlemen, thank you for joining today. Welcome to the BC meeting here in Kuala Lumpur. It's good to have everyone here.

The agenda is up on the screen. I need to warn you in advance that my laptop is not working properly so I may have to have Steve help watch the queue. But if I don't see your hand in Zoom, Steve is going to help out so that we can manage the queue. All right, the agenda is up on the screen. Does anyone have any additions or corrections to the agenda as presented? Okay.

All right. We have one hour's time for the meeting today. We have a couple of guests with us, Greg Aaron from Interisle is here and Jamie Hedlund from ICANN Compliance is here. Greg is going to give us a quick presentation of recent findings of Interisle research. And then Mark Datysgeld, one of our councilors, is going to take the chair. He and Jamie are going to lead us through a discussion on some ICANN Compliance matters. Then we'll have a policy update from Steve, and then we'll have a couple of issues to cover under AOB, including Lawrence's election calendar. Okay, very good. Again, anything else to add to the agenda? Anyone? Okay. All right. Very good.

Greg, welcome to the BC meeting. Thank you for coming. I'm going to turn the floor over to Greg. I believe you have some slides and then we

will have an opportunity for some Q&A. So the floor is yours, Greg, please.

GREG AARON: Thank you very much, Mason, and thanks to the BC for having us here today. I'm going to present the latest phishing landscape report, which is an annual report that I and my colleagues at Interisle have been producing. If you can go to the next slide.

You can read the full report and also a summary at that URL or you can just go to interisle.net. The reports are actually quite extensive. But I'll give you some of the highlights today and those things that might be most relevant to our work at ICANN.

We looked at a year's worth of data. So we captured phishing information from some widely used and reputable sources to see what happened over the course of a year. Those sources are the Anti-Phishing Working Group, OpenPhish, PhishTank, and Spamhaus. All of these sources are used commercially and by governments. In one way, yes, they're blacklists or block lists, but also we're looking basically at lists of confirmed phishing. So these are URLs of confirmed phishing attacks.

We're able to collect more than 3 million URLs or reports during that time from these four sources. That boils down to 1.1 million separate and unique phishing attacks. And by an attack I mean a phishing site, so a place that consumers are being lured to. So that means we saw a phishers launching 1.1 million phishing sites across the Internet.

That's a lot. To launch those, about 850,000 unique domain names were used, and I'll get into exactly what that means. Next slide, please.

The trend is, unfortunately, upwards. Now, we've been using these four sources as our baseline consistently over the last two years. They each collect their information and are sourced a little differently but consistently. So one of the implications is that either they're getting a really, really a lot better at finding phishing or there's just more phishing. We think, because they use consistent methods, what we are seeing is a general increase in the number of phishing attacks that are taking place and it is roughly doubled over the last two years, which is, of course, a concerning trend.

Phishing in a lot of ways is a low tech kind of thing to do. It mainly relies on people being fooled. It's a social engineering attack. But what we're seeing is it continues to work. People still fall for it despite all of the measures that are taken to protect people from it. What we also see is it wouldn't continue to happen and perhaps even grow unless it was effective. People do this to make money, and if they weren't making money, we would see a decrease. We may see an increase in number of sites because so much effort is used to take them down, and so they need to launch new ones all the time, but it's still happening.

STEVE DELBIANCO: Would you take one clarifying question, Greg? It would help us a little bit. We had this discussion with Graeme Bunton about the nomenclature between attacks, sites, and URLs. You've already used

the terms differently on the two slides so I'm confused. If Wells Fargo—somebody sets up Wells Fango as a domain name and they have a dozen or so URLs/ online banking, etc., and then they send 50,000 e-mails out to try to fool people to come there. Is that 50,000 attacks or is it a single attack because they use the domain Wells Fango? Or what about the dozen URLs that were involved? How do we map that to the numbers you're talking about when you use the word "attacks"? Thank you.

GREG AARON: Thanks, Steve. The number of URLs really doesn't matter. It's a meaningless statistic. Different phishers advertise, sometimes they send out a million e-mails. All of those may have a different URL and then that's personalized because that's how they get it through the spam filters. URLs don't matter. There are methodologies for looking at URLs and collapsing them into an attack. We talk about that in our reports and a lot of other people who study this do it the same way.

So, attacker site, there's basically synonyms, the way we use them and the way like the APWG uses them. That's what really matters in the end. Is it a place that you can go? Is it a place as advertised? And an attack often has multiple URLs associated with it.

STEVE DELBIANCO: And the number of attempted victims, the number of e-mails when e-mail is used, and it isn't always used, I get that. But the number of e-mails they send out trying to draw Wells Fargo customers to the Wells

Fango attack site, is each of those e-mails considered an attack? Or is all that just one attack?

GREG AARON: The e-mails are not considered attacks. Okay. So let's go to the next slide.

So where does the phishing occur in the domain name space? Well, the most domains used are in .com, although we would expect that because .com is so big and it's kind of a default and ubiquitous place for doing things, and it's always been that way. In the last year, .cn was used for the second most number of attacks, and then .shop and .xyz. And then you see .tk, .ml, .ga, and .cf. Those are repurposed ccTLDs run by a company called Freenom in the Netherlands, and they give away free domains. They just like free. They like a lot of free services, not only domains, but also hosting and DNS services. One is because they're free and they don't have to risk getting caught with a bogus credit card. Also, it allows them to launch a lot of attacks. Free services, by definition, don't spend a lot of money on other things like security and anti-abuse, so they're vulnerable places. So seeing those kinds of TLDs are not a surprise and continue to be a problem. Next slide, please.

We looked at gTLD domains. We did this because we can get the registry WHOIS and we can see where the domains were registered and see the registrar of note. We can't do that with ccTLDs as easily. But among gTLD domains used for phishing, 56% of them were sponsored by just 10 registrars. NameCheap at number one, GoDaddy

at number two. GoDaddy, of course, has much larger portfolio. NameSilo at number three. It's very common in this world for a lot of problems to be concentrated in a relatively few places. So here we see the majority of our problems in the gTLDs at least at a few registrars and even bigger numbers clustered to kind of near the top. Next slide.

Now, among the gTLDs, on the left side you see—well, actually, among all TLDs, you see a market share on the left. So ccTLDs about 39% of all registered domains, .com and .net represent about 48% of all registered domains. The new gTLDs are about 8% of registered domains in the market. However, when you look at the domains used for phishing, the new gTLDs are 26%. In other words, they're disproportionately represented for phishing. There are reasons for that. Part of it has to do with price, we are sure. A lot of the new gTLDs have always competed on price. So, low prices are something again that phishers like. The ccTLDs are 36%. But that also includes those free non-TLDs. If we back to those out, the percentage of ccTLDs use for phishing would be about 22%. So again, we've got some concentration in certain places. Next slide, please.

One of the things we should really keep in mind when we're looking at Internet abuse and phishing and so forth is the use of maliciously registered domains. Maliciously registered domain is a domain that the criminal went out and bought or obtained themselves. They did it for the purpose of phishing. These days, most phishing occurs on domains that were registered by phishers. They went out and got it, 69% in our estimation. There have been some other parties who have done similar studies. They arrive at about the same percentage. We

published our methodology and you can compare it to how some other people do it. So we think this is pretty close.

Most maliciously registered domains, it turns out, you can identify them with a relatively high confidence if you know how to look. There's a section in our report about how quickly phishers use their domains once they register them. It's pretty consistently that most of these are registered and then use within 7 to 10 days. The phishers do that because they don't want to get caught, they don't want the registrar to figure out they've got a credit card chargeback and canceled the domains, and that kind of thing. So that's one of the indicators.

Also, these domains often tend to get registered in batches. They usually have strings that have some telltale information in them. A lot of them actually are kind of randomized strings that don't mean anything. A person wouldn't be using them normally to have people visit their site. Not a lot of these domains have a brand name in them, actually, or a misspelling thereof. It always happens. But a lot of companies, especially large ones that are well resourced, are looking for those kinds of domains as they're registered and they start to show up in zone files. Phishers know that using the brand name in the domain itself is something that may attract attention. So instead, they'll put the brand name down in a subdirectory or a done in the path of the URL where somebody might see it and get fooled by it but it's not in the registered domain name.

Maliciously registered domains are really important because the registrar or the registry operator can suspend them, and they can do

so without causing collateral damage. When you go suspend those domains, the only person who's going to get hurt is the phisher, and that's what we want, and that's fine.

The other 31% of the domains that were used for phishing fall into two categories. One is compromised. So phishers have always gone out and found vulnerable website hosting, and then they'll put a phish on there. So the phishers appearing on an innocent party's domain, you don't want to suspend that domain because that would also take down that party's e-mail and their website. There you want to go to the hosting provider. They can take out the phish without bringing down the whole domain.

But at this point, the compromised domains are a definite minority of the phishing. It didn't used to be that way. Ten years ago, it was flipped. So we've got a situation in the industry where most of the phishing is taking place where the hosting provider can kill it but also the registry or the registrar can kill it. So that's important for people to know because you can't approach all three of those, and in my personal opinion, all three of those parties also have a responsibility to look at that problem and act within the responsibilities. Of course, every hosting provider, every registrar and every registry operator have a policy against phishing and similar illegal activities. They do have the right under their Terms of Service to suspend those domains. Next slide, please.

Of the maliciously registered domains that we looked at, over a third of them are in the new gTLDs. Again, the new TLDs are placed where there's what we would call churn or turnover. The renewal rates may

not be as high in some of those TLDs as they might be in places like .com, which has a lot of mature domains and a lot of mature websites. Next slide.

Of the gTLDs with the highest malicious registrations, we often found that there were very few compromised domains in them. So the top 10 are on the screen, they're all new TLDs pretty much except for .info, .com, and .net down at the bottom. But what we found is when you have a new TLD and they have phishing domains, almost all of them are maliciously registered, a high percentage ranging from 85 to 99%. Again, things that the registrar and the registry operator can go after.

The registrars in particular are in a good position to look at these domains and suspend them because they also have data like the WHOIS data or the registration and registrant information, and the billing information that nobody else has. That's really valuable information to help figure out if it's a legitimate registration or not. They're the only ones who possess it, especially now that WHOIS data is much more difficult to come by for everyone else. Next slide.

The other problem that we have are subdomain services. 13% of phishing took place on what we call subdomain services. So these are places where you don't get a second level domain, you get a third level domain. Some of these are hosting providers and they make free hosting available so you get a third level domain on a domain name that they own and operate. Some are DNS providers. In this category, we might include Cloudflare. They're not exactly a hosting provider but they're a proxy service, and so you put their name servers on your domain.

There are literally hundreds of these services but they're attracted to phishers because usually they're free. And again, the vetting process for getting these is slim to none. Some of them don't even require you to provide an e-mail address in order to get a subdomain. And then there's no WHOIS for them. Really, the only place you can go to get a phish mitigated is the provider itself.

So some of them are hosting providers like Hostinger. They will have domains on 000webhostapp.com. Those are very common. Some of these are operated by some large companies like Google runs blogspot.com, which you can build a blog and they will give you a third level domain. Well, phishers like that and they go get those. Cloudflare runs proxying service on trycloudflare.com. So you can get a third level domain there. DuckDNS is DNS provider. And then there are services like My.id, which is a place where people can get a third level domain if they don't want to register a second level one.

Some companies who are victims of phishing see a lot of this. Ironically, companies that spend a lot of money on dealing with phishing and they spend money on brand protection. Because normal domains they can monitor but you can't monitor these as well. Again, there's no WHOIS and you just have to find them after the phishing starts to happen, which is a real problem. So let's go to the next slide.

38% of the phishing attacks we've studied were just 10 hosters. Cloudflare is not exactly a hosting provider but they do provide the path through proxy service so their name servers are used. They were definitely the most prevalent. People like them because they provide DDoS protection. But phishers also like it because you can't see where

the hosting actually is. Because the relocation of the hosting is hidden behind Cloudflare is proxying service. Microsoft is on that list because they have a few of those free providers who use their hosting, so don't read too much into that one. Same for Google and Amazon. Next slide.

The hosts with the highest scores are up on the board right now. NameCheap is not only registered but they're a hosting provider, and they had a lot of phishing given the number of IP addresses in their AS. That's the ranking we see there. We'd like to use that metric. Some people operate a large number of IP addresses and some relatively small, so this is a way of kind of normalizing it to the size of the business. So again, a lot of phishing concentrated in some relatively small numbers of places. Next slide.

So the takeaway I'd like to leave you with is that these numbers are a floor. These are the ones we were actually able to count but there's a lot more phishing that isn't captured. I'll give you an example. Meta, which is the company that owns Facebook and Instagram, filed a lawsuit in December. The lawsuit said that they had recognized and captured data about 35,000 phishing attacks at one of these third level providers, ngrok.io. So they went before the court and said, "We have information and screenshots, about 35,000 of these, and we want to figure out who the phishers are." When we looked at our data, we only saw about 800 of those that showed up in our data out of 35,000.

That's probably an extreme example. But a lot of phishing is not captured because some companies that don't share the information about the phishing that they suffered. They're worried that if they do, their users are going to feel like the service is unsafe and they won't

use it anymore. Generally, companies don't share a lot of information. That's the same with financial fraud and other things. So there's a lot we don't know. We're just counting what we can count. But there's a lot more out there that we should be worried about. Majority of the problem does tend to be concentrated in a small number of providers. So if you're a brand owner, you have to figure out where those are and you may have to establish relationships with the providers who are providing the resources that phishers are using against you.

Mitigation speed is important. Once you find out about a phish, you want to get it down so you decrease the number of victims. But what we're seeing is that's Whac-a-mole. The phishers will just launch more attacks. So prevention at these providers is important. What we would really like to see is some of them get a better handle on why the phishers are getting into their systems over and over and over again, and have them hopefully do a little better job of detecting this stuff on their platforms and their systems before it becomes somebody else's problem.

Finally, malicious registrations are a way to deal with the problem. The hosts and the registrars and the registries can share in the responsibility for seeing those things, hopefully proactively, and then taking them down. So that brings us to the end of the slides. We do have a little bit of time for Q&A.

MASON COLE: Greg, thank you very much. I appreciate the information and that's helpful, especially informing our work on DNS abuse which the BC has

been championing for some time now. So I'm going to open the queue. Raise your hand, please, in Zoom if you'd like to pose a question to Greg. Let's go to Steve. Go ahead, Steve.

STEVE DELBIANCO: Thanks, Greg. The fourth takeaway point that can be identified, did your report go into some methods by which the name itself can be identified as a malicious registration just by the nature of what characters are in the name? Or does one have to look at the underlying content at the site, or wait for a report to come in from the company whose customers are being victimized?

GREG AARON: Yeah. So we do have a section on methodology. Then some similar studies have been done by the University of Delft and some other places. But basically, you need to look at a few things like how young is the domain? Does the domain make sense to a person? Or is it composed of random characters and nobody would be able to use? If you look at the entire URL, then do you see evidence of a brand name in it? That's a red flag, and a few other factors.

I also see clusters of these. So when you see one domain name, you'll also see a whole set of domains registered literally at the same time at the same registrar using the same name servers, and you start to see phishing on them. Sometimes those clusters can be large, hundreds to thousands of domain names at a time. I encountered one the other week of 1200 domains. Once you start to see that, they really stand out like a sore thumb.

So we have a scoring mechanism that looks at various factors. But operationally over the years, I've dealt with this over and over again, and you start to see things that look really suspicious and really obvious. Then if you're at the registrar, you can then look at, "Well, who's my customer? Is their WHOIS information accurate or plausible?" They have some other clues they can use.

STEVE DELBIANCO: Is all of that capable of being automated into an algorithm or heuristic, or does it require a human examination to—

GREG AARON: It can be automated and there are heuristics. One thing you do is, yeah, you compile a list of brand names, for example, as part of that heuristic.

MASON COLE: Thanks, Steve, for the question. Crystal, please.

CRYSTAL ONDO: Thanks, Mason. Crystal Ondo for Google. We sit on the BC but we also on a registrar. We have been on the Interisle report. We were no longer, thankfully, on the Interisle report due to a lot of actions. But I just wanted to point out I think in the answer there, a lot of registrars do not automate. I would argue that almost all don't because there are so many factors that you have to look at and the fact that 31% are compromised domains. It's a huge risk to automate to take down

domains. I often say it's an art, not a science, because if you see it a lot, you've been doing this a lot, you can spot it very easily. If you're a new agent to this, it's harder. So I just want to make clear that you could automate but most registrars do not.

GREG AARON: In fact, I'm aware very few who automate to none, because you want this stuff to go through a member of your Abuse staff who make a determination, and you want to avoid the false positives. So that's kind of the industry standard. There is a proactiveness that is still missing in the industry where a lot of parties wait to hear about a complaint and then they take a look at it.

What I would love to see is some processes going on in the background. I know, for example, at GoDaddy, one of the ways that GoDaddy finds stuff is by looking at the financial information, about the billing information, which is one of the reasons why GoDaddy has a lower rate of abuse in general, especially given their size than a lot of other registrars.

So to your point, Crystal, you want to have somebody look at, for sure. But also keeping the bad guys out is good for business for everybody. Thank you.

CRYSTAL ONDO: I'll clarify, fraud prevention is automated. That's a different issue. So when you're dealing, especially with new gTLDs or including com, net, legacy, you have five days as a registrar to delete it, and you could still

get your money back. So if you're trying to prevent chargebacks, which definitely impacts your abuse numbers, that is an automated process. So they're treated separately.

MASON COLE: Thanks, Crystal. We're going to go to Vivek, and then we're going to cut the queue after that because we're running behind on time. So, Vivek, over to you, please.

VIVEK SENGUPTA: Thank you for the presentation. Very informative. Did you see any data on IDNs being used for phishing attacks? Thank you.

GREG AARON: Yes. We have a section in the report where we actually counted them and looked at what was going on there. IDNs are not used for what we call homographic attacks very much. So that's where somebody tries to fool you by creating a domain that looks like a brand name like microsoft.com but uses an IDN character with an accent or something. It happens but not very much. What we actually found is probably one party out there did some during our study period, and it was somebody who was phishing some cryptocurrency companies. So the homographic attack is something that exists but it's pretty rare. IDNs, for the most part, are not used extensively or an unusual number for phishing.

MASON COLE: Thank you, Vivek. One last question. Go ahead, please.

[NISHA PRAKASH]: I'm [Nisha Prakash] from Sky. I just wanted to touch on two things that I saw in your presentation, one being registered domains should be suspended by registrars and registries, and then your subdomain setups. Something we struggle with is where the infringer or domainer will register a very generic domain. So working for a media company, they would register, ilovetv.com. And then they'll create the trademark at the third level, which would be skycinema.ilovetv.com. Now, when I go to register or raise the abuse, it won't be reacted to because the actual root domain doesn't contain the trademark. But the trademark sits at the third level. So we will never get a takedown in that instance, and it's a huge problem for us because they're just creating that abuse at that third level but the domain is generic. So why are we not getting reactions? How do you get around that?

GREG AARON: It depends on the nature of the complaint. If the complaint has been made based on an intellectual property issue then you won't get the response you want because the second level domain doesn't contain the trademark. So an effective thing to do is to say, "This is phishing." Yes, it's at the third level but your hosting providers really should take down that phish, if not the entire domain. We should talk separately about some methods. But the complaints need to be specific about what the problem is and what the situation is so you can convince the

hosting provider of the problem and what the appropriate response should be.

[NISHA PRAKASH]: Yeah, we could catch up on it. Thank you.

MASON COLE: All right. Thank you very much for the question. All right, folks, we're a bit behind on time so I'm going to cut the queue now. Greg, thank you very much for being our guest today and thank you for your presentation.

GREG AARON: My pleasure. Thank you.

MASON COLE: All right. Thank you very much. All right, ladies and gentlemen, I'm going to turn the chair over to Mark Datysgeld for just a moment and he's going to lead us through our discussion with Jamie Hedlund. So, Mark, can I give you the floor, please?

MARK DATYSGELD: Thank you very much, Mason. It's been a pleasure receiving our guests from Interisle. Now I turn to our friends from Compliance. I would like to highlight that Compliance has actually been super forthcoming with the DNS Abuse Small Group from the Council. So thank you for

that. This has been greatly enhanced. This cooperation that we're building is something that I feel benefits the entire community.

We set some questions ahead of time based exactly on that experience. So these questions are not just pulled out of thin air. It's questions that are kind of remaining from our work in the DNS Abuse Small Team. And we want to use this venue that the BC is providing to actually maybe air these questions and bring some reflection to the community and hope get some insights from Compliance into how to move forward. So without going much further than that, should we do like a brief introduction of who Jamie is?

MASON COLE: Yes, please.

MARK DATYSGELD: Jamie, could you introduce yourself, please?

JAMIE HEDLUND: Sure. Thanks, Mark, and thank you for having us. I'm Jamie Hedlund. I'm head of ICANN Contractual Compliance. I'm here with Roger Lim, who is the head of our Singapore office for Contractual Compliance. He's also one of the leads on DNS abuse. He is going to try to answer the questions that were raised.

We sent around a couple of slides before the meeting to provide background data on what Compliance is doing in the realm of DNS abuse. I'm not going to go through that here. It's data, but if you have

questions about it, please feel free to ask those. With that, I'll turn it over to Roger unless you want to—go ahead. Okay, so with that, I'll turn it over to Roger. Thanks.

ROGER LIM: Hi. Good afternoon. Roger Lim for the record. Do you want me to read out the questions, Mark?

MARK DATYSGELD: Sure.

ROGER LIM: So first question is what is Compliance's view on one of the key items highlighted by the small team on DNS Abuse draft report, Maliciously Registered versus Compromised Domains? Could this distinction be leveraged to combat abuse moving forward? So there was a question. So in response, basically, Compliance reinforces all obligations in ICANN's policies and agreements. The obligation in Section 3.18 of the Registrar Accreditation Agreement refers to reports of abuse involving registered names sponsored by registrars, including reports of illegal activity.

In the course of an inquiry for registrar, based on these abuse complaints that we receive, some registrars may indicate that the domain was compromised. But this is not a specific data point that we request, consider, or track, because the RAA does not make distinctions between compromised or maliciously registered domains.

MARK DATYSGELD: Let me make this dynamic. We can do question and answers. No, that's great. This dovetails into what we were discussing. We just saw that the prevalence of malicious registered domains as a source of phishing, and I think this just goes towards showing to the community that we need to bring those statistics to the actual process. It's good to know how Compliance is looking at this right now, because if it's not being tracked, then it's something that we as a community should seek to have tracked. So that's what I think is important right there.

The follow-up question actually was mentioned in the previous presentation as well, which is bulk registrations. We were talking about this a lot in the small team but it's something that we realized we don't know a lot about. So our question right now is how prevalent is bulk registration, if there is insight into that, and if Compliance has any idea of whether that behavior is somehow impacting DNS abuse? Are those data points that we have or have insights on?

ROGER LIM: Thanks, Marc. Again, it's something that Compliance does not track or maintain information on bulk registrations. On occasion, we do receive complaints involving large numbers of domain names could be abuse-related or it could be something where registrant has a portfolio of a large number of domain names regarding renewals, for example. But again, we do not track information on bulk registrations, and basically, we enforce the obligations pertaining to the complaint and all domain names involved. So we do not actually distinguish

between individual about registered domain names because the policies and agreements, again, do not make that distinction.

MARK DATYSGELD: It's good to note that some of the information we might want are things we need to ask. This keeps pointing towards the need for the community to get started thinking about what data do we want, right? This follows into something that we have heard from you individually during our meetings, but it would be good to discuss this with the broader community. How does Compliance feel about the abuse reports that reach you? Are they actionable? Are they complete? What do you feel about the quality of these complaints? How they have been evolving over time? And what could we actually do to better inform our clients of best practices? What are we looking towards? How do we actually get the people to get those complaints in the best way possible?

ROGER LIM: Thank you, Mark. We do receive many abuse complaints that do not result in cases that we can initiate with the registrars. Just quick data point, from June 2021 to May 2022, we closed about 3600 invalid complaints. In approximately 70% of these complaints, there was no evidence that the sponsoring registrar was ever contacted prior to filing the complaint with us. So if the registrar never received the abuse report prior to filing the complaint, there isn't something that we can investigate. Sometimes it's also a misunderstanding of our Compliance role and sometimes the complainant believes that they

can report the domain to ICANN Compliance and then ICANN Compliance gets it deleted or transferred or something like that. So there might be some misunderstanding of what we can and cannot do.

In approximately 10% of those cases that I mentioned earlier, the domains were already suspended. And when we do close these invalid complaints, we do not just close it and just say, "Thank you. Bye." But we actually provide information on where the deficiency is and where applicable, provide additional information to help them with how do you file abuse report, where do you get information on where to file an abuse report with. Then sometimes, if the complaint is about ccTLD, for example, we actually provide information to them on, "Hey, this is where you can contact the ccTLD directly so that you can actually follow abuse report with them directly." We do try and provide this additional information as much as possible to all this complainants when we do have to close them so that they do not feel like they lost, basically.

We do encourage reporters of DNS abuse to review the guidelines published by the Registrar Stakeholder Group that's available online on their website. Even though these guidelines are not enforceable by the Compliance team, they do provide information that's useful in how to file abuse reports with the registrars and what kind of information that would help the registrars perform an investigation. That's all the stuff that we've been doing. Thank you.

MARK DATYSGELD: Thank you. Interestingly, you will find in our final report the word "reporting pipeline". That term appears there and it seems like we need to start making people aware of the reporting pipeline and how to get the information to where in order to optimize our processes.

The next question is actually raised something that was brought by ALAC in their comments to our team. It just raised my attention. Us from the business sector know a lot about Know Your Customer practices. It's a hot term. But this is not something that we hear a lot in the ICANN realm. We don't hear a lot about KYC practices. So this is more of a personal question, if you would. What's the impression of Compliance on the potential impacts of Know Your Customer practices? Could we implement that? Would that be helpful? Can we leverage that sort of practice to reduce abuse rates?

ROGER LIM: It's actually not our role to opine on the relative merits of providing possible changes in policy or contractual obligations. We have in the past and will continue to provide feedback to small teams in response to direct requests and through the metrics that we publish on a monthly basis. This includes information and data on the complaints that we receive that can help inform ongoing community discussions, such as those that are related to abuse in particular. We also provide input and feedback on the clarity and on enforceability of any new obligations to ensure that we are able to enforce them. Thank you.

JAMIE HEDLUND: If I could just add to that, as you all participate in policy development and implementation, a key issue for us is the clarity and enforceability of any obligations that ensue. It does not want any good if there's ambiguity or lack of understanding or people have different beliefs on what is actually in the policies or agreements. To the extent that when you're participating, you can really push for clarity. We will, in the background, also provide our own input in terms of whether it's on SubPro or this or Temp Spec on whether we think that there's an issue with either the clarity of the obligation or its enforceability. Thanks.

MARK DATYSGELD: I have a final pre-prepared question and then we will give the opportunity for BC members to ask questions. The final prepared question is: are there threats—existing or potential—that Compliance would like the community to look towards when discussing DNS abuse in the coming years? Are there trends that Compliance would like to make us aware of as we move forward with this work and as we intensify this push? Any suggestions, basically?

ROGER LIM: Basically, from a Compliance perspective, the biggest issue that we see is ensuring that there is a community-wide understanding of what the current obligations are and also the role of Compliance in enforcing them. That would be the biggest thing that we see. Thank you.

MARK DATYSGELD: Thank you very much. I throw it back to Mason so that questions for BC members can be opened.

MASON COLE: Mark, thank you very much. Caroline, let's go to you, please.

CAROLINE GREER: Great. Thanks so much for this presentation. Greg, in his earlier presentation today, discussed the importance of speed in mitigating DNS abuse by maliciously registered sites, as well as a number of strategies in identifying maliciously registered domains, such as if a whole batch has been registered together if they're using odd strings of words and terms. I'm wondering if ICANN Compliance has a role in helping registrars identify maliciously registered domains and what kind of challenges might you see in speed in negation, as Greg mentioned.

JAMIE HEDLUND: Thanks. There's no explicitly—call that role for Compliance to engage. Obviously, we follow up on complaints and we also do proactive enforcement. When we hear about things, we will reach out. But the agreement is what the agreement is. So when we get complaints or we find out things, whether they're an individual names or bulk registrations or the large number of names, we try to immediately go after them. But I also understand that the perishability of these names and that creates an issue for enforcement.

MASON COLE: Caroline, thanks for the question. Steve?

STEVE DELBIANCO: Jamie has mentioned earlier that Compliance, through your experience, you understand more than anybody in this community. Which elements in the agreement withhold you from being effective at Compliance? Weasel words like reasonable or missing terms that are explicit. Because I wonder whether as the DNS abuse work proceeds, would we be able to present potential changes in language to your department? You could comment on ways to make it even tighter so that you'll be more effectively able to enforce it later on. Will you be allowed to participate in that process?

JAMIE HEDLUND: Sure. Thanks for the question. We do participate in the process. We do provide feedback as part of ICANN Org. Again, as I just mentioned, our real focus is not on what policies are better than others or what changes would be more effective, but really on the clarity and the enforceability of them. So if we get presented with something that when reading sounds interesting and great but really leaves us no clear method to enforce either because it's ambiguous or because there's just not clear understanding of what the issue is, we are not the first place you go to ask whether we think this would be a good idea or not.

MASON COLE: Okay. Thanks for the question, Steve. We've got time for one more for Jamie and Roger, if there are other questions, and then we're going to draw a line on the queue. Anyone else? Okay. Jamie, Roger, thank you very much for coming. I appreciate you being the guest of the BC today.

JAMIE HEDLUND: Thanks for having us. Our door's always open. Please stay in touch.

MASON COLE: All right, thank you very much. Mark, thank you for leading that part of the agenda. All right. We're going to go to item number four. Steve, take the floor, please.

STEVE DELBIANCO: Thanks, Mason. Your policy coordinator role is what I fulfill in the BC. On most of our BC calls, which we hold every two weeks, at least half of the meetings are taken up by running through the policy calendar and then debating among BC members how we want to approach a certain item, how do we want to prioritize it. We're not going to do that today. It's an open meeting. We are short on time and Lawrence has some things to cover.

I simply wanted to say that if you look at the policy calendar I circulated yesterday, you'll see that after a relatively slow summer here in the Northern Hemisphere, we now have seven open public comment opportunities in front of the BC. I'm happy to say that we have volunteers for several of them. Vivek and Olajide, Margie, thank

you for that. But I need volunteers to help with several items that are in the policy calendar, numbers four and five, number six, and number seven.

I would suggest taking a quick look at that, finding something you can help with over the next month and a half. As I always do, I'll assist by pulling together previous BC positions and resources that can be drawn upon. I'll handle the editing, the formatting, the submission and coordination as I always do. This is a super opportunity. We're very busy in the next two months.

I'll also suggest that in the last two days, I've circulated several e-mails, Caroline has as well, on the two topics the BC is paying a lot of attention that you're in Kuala Lumpur. The SSAD Light, the ticketing system, we had a significant role of getting that moving. And the other is the DNS abuse which we spent most of the last hour on. On both those topics, we need a rigorous discussion as we look to October when Council will probably have to vote on what to do with the SSAD. Mason, that's all I have right now. I'm happy to answer your questions or toss the ball over to Lawrence.

MASON COLE: Thank you, Steve. Questions on the policy calendar for Steve? We do need some volunteer help. So anyone who can raise their hand and give your leadership team an assist would be very much appreciated. Questions or input for Steve? Okay, queue is clear.

All right. Let's move to AOB under the agenda, please. I'm going to go straight to Lawrence before we open up the floor for the rest of AOB. Lawrence, over to you.

LAWRENCE OLAWALE-ROBERTS: Thank you, chair. I hope I can share my screen. Otherwise, the major information that will need to be passed to members is a notice on the forthcoming BC officers' election. We are looking to open the process. Start with following the Bylaws, we need to provide the two-week period for members to nominate members into any of the four officers position. The positions open: the chair, vice chair for Policy and vice chair Finance Operation as well as CSG. Thank you, Mark. Great.

We're going to be opening the nomination period from Monday, the 24th of October. It's going to be open for two weeks until Monday, the 7th of November 2022. Members who have been nominated or who will be nominated into any of these propositions will need to provide a candidate statement, which will be shared on BC private on or before the 14th of November 2022. We have a Candidates call on the 17th of November, which also happens to be the second Members meeting in November. While our Members meeting start by 15:00 UTC, the Candidates call will start an hour earlier, which will be 14th of November 2022. The next day will be Friday, we will send out ballots to all financially paid members of the Business Constituency to start voting.

The voting links will be open for the week and we will be closing this by Thursday, the 24th of November. The candidates who will be taking

their offices from the 1st of January 2023 will be announced on the BC private list by the 25th of November. So we have two weeks for nominations. The week after will be for the Candidates call. And thereafter, we will start the voting proper, which will be open for a week. We want to invite BC members to nominate persons that they feel are qualified for any of the four officer positions when we open this process on the 24th of October.

Please note that I'm happy to say also that well over 80% of our standing members are paid up and financially up to date, if not more than that. So majority of BC members will be able to cast a vote and will also be able to be nominated during this particular period. We should definitely look forward to having this information on the BC private list. I'm sure that it's going to be a very active election period for us.

Secondly, I want to use this opportunity to also thank all the contributors to the BC newsletter, ICANN75 newsletter. I'm sure all members have taken time to go through. It's a beautiful piece. Thanks to Mason and the team for their articles. We are looking forward to— Imran, thank you also for all the efforts made. We want to encourage members to keep up these forms of activity. Thank you. I'll yield the floor back to you, Mason.

MASON COLE: Lawrence, thank you very much. Excellent work on the newsletter on your part. Thank you for all your help on that. Okay. All right. Friends,

we're at the top of the hour. Is there any other business for the BC before we adjourn?

I have one other issue. On the officers elections, if anyone here is interested in standing for office or would like more information about how to go about that or what's involved in holding a BC office, feel free to approach Steve, me, Marie, Mark, Lawrence, Tim Smith. Any of us can give you more information about what's involved and how you can contribute. So feel free to approach any of us about that. Mark?

MARK DATYSGELD: I have a small AOB. The schedule is not too bad right now, so if after we come to a close, the BC members would like to just mingle a little bit around. It's been so long since we have been together. So if anybody wants to just shout out, let's huddle here post meeting and have a chat.

MASON COLE: Good idea, Mark. We might want to take that out into the hallway because I think somebody has the room at 4:30 after us.

MARK DATYSGELD: I mean, on the hallway, of course.

MASON COLE: Okay. Any other business for the BC this afternoon? Marie, did you have anything?

MARIE PATTULLO: I'm always happy to mingle if Mark's leading the mingling. In all seriousness, if you don't know me, I'm Marie Pattullo, the one that sends you boring e-mails about Council. And if you do want anything, Mark and I are here for you. Thank you.

MASON COLE: Marie, did you want to say something about volunteer for Applicant Support?

MARIE PATTULLO: Yes. Very briefly, whole process going through but there is going to be a small group of people who are going to try to figure out how to get Applicant Support for the new round up and running as soon as possible. I'll send you more details on the list. It will be one person from the CSG. We need to identify that person before next Monday. We need somebody who's got SubPro experience and somebody who actually knows what an applicant needs and preferably has Applicant Support experience. Thanks.

MASON COLE: Okay. Thank you very much, Marie. So if you're interested in that, please approach Marie. All right. Other business for the BC? Okay.

Happy birthday again to Brenda. Thank you again for all your support. Thank you, Brenda and Terri, for your support. The BC is adjourned. Thanks, everyone.

[END OF TRANSCRIPTION]