ICANN82 | CF – Joint Session: CPH and CSG Work Session
Sunday, March 09, 2025 – 16:30 to 17:30 PST

SUE SCHULER

Hello and welcome to the CPH and CSG Membership Work Session. My name is Sue and I'm the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom.

On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. I will now hand the floor over to Beth, Owen, and Mason.

OWEN SMIGELSKI

Thank you, Sue. My name is Owen Smigelski. I'm with Registrar Namecheap and I'm also the Chair of the Registrar Stakeholder Group. So, first I want to welcome everybody here and also thank our colleagues in the CSG. This session came out of some discussions that had kind of like over drinks or whatever with regards to what goes on with DNS Abuse reports and what kind of struggles do some reporters have and what do registrars have.

And so, we collaborated where the CSG has come up with some examples of reports that they thought should have been actioned and then the CPH has come up with examples of spurious abuse complaints that we received so you can kind of get an idea of the kind of things that we see. So, we're going to get into this after I think, Mason, you're going to say a few words.

MASON COLE: Yeah, thanks, Owen. Good afternoon, everybody. Mason Cole here, Chair of the BC and also taking my turn as Chair of the CSG. I want to echo Owen's thanks to everybody in the room and particular to our Contracted Party friends for making time for this session. This is a good opportunity for us to increase our understanding of the abuse process from a Contracted Party side and I hope we all come away smarter and better equipped to handle DNS Abuse.

So, Owen, Beth, thanks for making time for this. It's going to be a good session and we're looking forward to it. In terms of format, my colleague Marie from the BC is going to lead, she's going to introduce each case and then I understand, Owen, that we're going to take a break and get some input from the Contracted Parties on each case and then we'll hand the meeting back to you. Sound good? Okay.

OWEN SMIGELSKI: Yes, that sounds good to me.

MASON COLE

So, if we're ready, then I'll just turn it over to Marie. Marie, over to you.

MARIE PATTULLO

Thank you very much. From the CSG side, again, thank you very much for being here. I'm really glad there are so many people in the room because it is so cold in here that I'm hoping that we're going to talk a lot and generate a lot of warm air and get closer together. So, as we explained already, the idea of this session is talking, understanding each other. So, from our side, we came up with some cases that we've come across in real life. Some names have been changed, obviously. Some have been generated by AI.

So, there's no naming and shaming here. It really is a session where we'd like to understand from you how we can all work better together. The running order, Vivek is going to present from the BC. Philippe will go through some stuff from the ISPs for us. I'm sorry, before Philippe, Chris and Cole have a second case in the BC, then Philippe from the ISPs and John from the IPC. So, I think the easiest is we just hand over to the guys. And please, after each case, let's get this discussion going. Thank you. Vivek?

VIVEK GOYAL

Thank you, Marie. Like Marie said, my name is Vivek Goyal. I run an online brand protection company called L.R. And out of many cases that I had, I pulled this one out. So, a company changes its branding. And as you can see, the branding is completely different. Now, what happens is a scamster would use an old branding,

create a page, put a login information there, and then solicit information and then use that information to scam people.

Now, we have filed complaint with the registrar in question here multiple times, but we have not received any response. One of the reasons we think is since there is no active website where the old branding can be viewed, there is no way for the registrar to validate whether this is a genuine branding or not. So, I would request some inputs from the experts here on what is the recourse that companies like us can do in this case. Thank you.

REG LEVY Thanks, Vivek. So, in this case, I was confused because I didn't realize that there was no example of the branding. Perhaps submitting a screenshot of the prior branded website would be an additional piece of data for the registrar. But in this case, honestly, I feel like you just get ICANN involved because this seems to me like a pretty clear issue of phishing. And so, I'm annoyed that the registrar hasn't acted and here we are talking about it. I know that your customer is even more annoyed than I am. But my recommendation in this case is report them.

VIVEK GOYAL Okay, thank you. And would a snapshot from like a web archive would suffice in this case? Okay. Thank you.

REG LEVY I would say that it would. Registrars may treat things differently. But in this case, you have a direct phish attack on a specific trademark, even though it's an older trademark. It's an older code, sir, but it still checks out.

MASON COLE We got a couple of hands up in the room here. Volker, you want to talk?

VOLKER GREIMANN Yes. I mean, when I look at this, the first question I would ask, what is the evidence that's being presented? Are there any screenshots? Is there anything that allows me to verify what is being said? I mean, for me, these are two unknown brands that I have never heard of. I don't know what happened in the background. You are saying that they abandoned this brand. Was this old trademark maybe picked up by a new company that is now providing services under that and they don't like that. Provide evidence to the effect of showing us, without doubt, this is phishing. I think the more you can give us to tell us that this is actually a case of phishing, the easier it will be for us as registrars to action those.

OWEN SMIGELSKI Thanks, Volker. And I'm going to jump in. This is Owen Smigelski. Just want to caution, though, you can give too much information. And that's really a thing. A lot of times, people processing these complaints, they have numbers, and they've got work they have to do. And when you come across a 35-page PDF with annexes and

stuff like that, it can be daunting. Really, we want, okay, why is this a phish? Screenshots, stuff like that.

And I didn't really realize this until I went to a registrar. But our customers, we're breaking our contract when we suspend the domain name. And so, they can, they will, and they do sue us over that. So, we need to have evidence that when this does legal demand from a lawyer or they sue us in court, which I was shocked when a customer sued us recently because I looked at it. I went, this is a clear-cut case of illegal activity. Why are they suing? But they do. And so, we need to be able to have that to defend ourselves. And it's not that we're just trying to be difficult. It's just we need to be able to have that and then be able to verify that. Thanks.

VIVEK GOYAL Is it a general practice that you would respond to the complainant and say, this is missing, or can you provide this? Or, because what we have received is silence. So, if you can help on that, please.

REG LEVY Yes, typically, we do say, we didn't see anything. We're closing the case. If you have additional information or additional evidence, please provide it. That's not required. A response is required. Request for additional data is not required. So, they may have sent you, not silence, but an autoresponder that says, hey, we got it, which is silence from your standpoint, but is technically compliant.

But yeah, we don't always ask for additional information. We typically just say, we don't see it.

MARIE PATTULLO

Okay, not seeing anyone else. So, if I could ask you to go to the next slide, please, and hand over to Chris and Cole. Thank you.

CHRIS LEWIS-EVANS

Yeah, good afternoon, everyone. Chris Lewis-Evans from Clean DNS. So for this example, a report comes in. It's a Brazilian bank, in Portuguese, if anyone wants to practice their Portuguese. The report says that this is a commercial company. They represent the entity, the bank here. And this site is being displayed and is phishing. However, as you can see, there is no credential capture within this page. Not in the report, but openly available is the fact that the domain is three days old and is on a content delivery network that the banking site is not on.

So, this was not actioned by the registrar. Just want to get a feeling about why not? What level would it need? Does it really need the credential grab when it's quite clearly not related to that entity? And especially in financial, could be used for phishing quite heavily.

REG LEVY

Could be, isn't. So, this is not phishing. This sure is a terrible use of your customer's mark. You say it is clearly not related to your customer or to their business. I don't know that. And my registrar has absolutely shut off banking websites because they were

reported by a customer or by a vendor of the bank. They reported their own customer site.

It looked like a phish to us because it sure did have a login site. We took it offline on a Friday night, and boy, did I hear from corporate counsel before Saturday morning. We don't know that it's not related to your customer. You do, but this is a trademark issue. It's just not phishing. Volker, go ahead.

VOLKER GREIMANN

Maybe just to provide a little bit more color as well. We've had cases where very well-known and respected registrars, corporate registrars reported domain names to us that allegedly phished or infringed on their customer site. And those were domain names registered through our corporate portal for our corporate customer that was a subsidiary of their corporate customer. And they operated their TLDs on a different platform.

So, basically, one side, one hand, not knowing what the other is doing is a real problem. And therefore, we need absolute evidence and certainty that this is phishing or a problem. And even if it comes from the highest corporate council of that company, they can make mistakes. And we need to be sure that we don't repeat those mistakes when we take action.

REG LEVY

I also want to say that use of a content delivery network may be evidence for you, but it's not necessarily bad. A lot of places use CDNs.

That's why they exist, right, to provide their content locally. And especially for a Brazilian or, I don't know, actually, if this is Brazilian or Portuguese customer, they may use a CDN specifically to provide their services to non-Brazilian, non-Portuguese accessors, because that's going to be faster than trying to get directly to their servers, which are local. So, for their international customers, that's why they have a CDN. I know that the large CDNs are also often misused. But they are also often not misused, right? That's why they exist, and that's why they're big.

OWEN SMIGELSKI

Yeah. Thanks, Reg. Also, Reg is not the only registrar around here. We are having a little discussion background that has suspended a bank's website on accident, well, not on accident, but based on a report, but it was an incorrect report. So, that's why we really do need to see that stuff there. But go ahead, Chris.

CHRIS LEWIS-EVANS

Yeah, thanks. I think this is interesting to pull out. So, what is clear on there? The entity is obviously very clear. There isn't a credential gap. You can see it's a newly registered site. So, impact could be lower. I'd still get, if you take down the wrong site, that's going to cause harm. If the report was just, as I said, which is what was

delivered in this case, what other mechanisms would you use to investigate this?

So, there's obviously hard to see here because you can't roll over a mouse. There're two buttons there. So, is this something that would be clicked on through the investigation to test that, if that hasn't been provided, or is it just based upon what's provided in that report?

REG LEVY

I'm going to say that the answer is going to be different for each registrar. If the person who's investigating this uses the Chrome browser and it translates those buttons, and one of them is log in, that's phishing. But as it is, if it's just like, learn more, contact us. I don't actually know what those buttons say. Sorry? Okay, so one says government and the other says business. Yeah, I don't know what to do with that. Go ahead, Volker.

VOLKER GREIMANN

During the course of the investigations, we will, of course, try to draw in as much information that we have available. So, when we get a complaint like that, and for example, we see that the domain is registered through a reseller that isn't providing corporate services to such clients, then we might take that into account. If the domain is very fresh, then that might allow a faster action than if that domain is already very old.

If it's a site for a Portuguese government side of a bank that's registered through a Chinese reseller, that might be an indication

that there might be something fishy about it. So, we try to draw in as many informations that are available to us that you might not have, but you should also provide as much information that shows to you that this is the case. And we might even reach out to our customers and say, here, this is a problem we have with this domain. We are tending to take action. We might not tell you that we have a 48-hour window where we want to expect a response. So, it might be looking to you that we are not providing response, whereas we are conducting internal investigations.

OWEN SMIGELSKI Thanks, Volker. Graeme?

GRAEME BUNTON Thanks, Owen. This is Graeme Bunton from the NetBeacon Institute. I think to pull up from this example and maybe offer some guidance to those trying to report abuse, and hopefully this is captured in some of the documents the Contracted Party put out today, but if you're reporting phishing, registrars really want to see evidence of two particular things. They want to see evidence of an impersonation of identity, that the website is pretending to be an entity that it is not, typically a brand, because those brands have value. And so, it's not just that that brand exists on the site, but the site itself is trying to be that brand.

And then the second piece is an attempt to gather sensitive information. And so, the screenshots you provide should demonstrate both of those things. And you might need to,

especially where it's being translated, draw particular attention to those details. And if you can do that, I think you'll have much better success than just a screenshot like what we're seeing here. Thank you.

REG LEVY: So, you also indicated the age of the domain was flagged in the report. This page doesn't have a whole lot of information right now. So, to me, this seems in line with a new domain purchase. It's a relatively rudimentary site. It's not like a full site that's ready and working right now. It's just sort of a holding page. Brands have different jurisdictions that they become active in. And so, it's not rare to see a new website belonging to the brand, possibly registered with a different registrar, because their local affiliate is spinning up, right? So, the age may be important for some things, especially if there is phishing. But without that, the age doesn't tell me a whole lot.

OWEN SMIGELSKI: Luc, you're next.

LUC SEUFER: And also, to add on to the complexity of the case, if, for example, you would be providing like proof that this domain name is used with another domain name for BEC or for phishing, we would also take action. But you have to provide the link, like Graeme said. You have to show the impersonation.

CHRIS LEWIS-EVANS

So, thanks. Can we go on to the next slide, please? And just to say, this is pulled out as an edge case. So, we'll work through it a little bit. So, I'm just trying to draw out some of these. And it's been really good feedback. So, thank you. So, this report was reported to the registrar. And they received a response that basically said, it's not phishing. It's a brand issue. Please contact the hosting provider or use UDRP. Summarizing that there. So, a report was made to the hosting provider. The hosting provider was non-responsive. Cole, do you want to talk about UDRP and the impact?

COLE QUINN

Yeah, I think for this room, it's going to be pretty obvious sentiment that UDRP is obviously much more expensive. And it takes a long time. And it's not scalable. And it's rather demotivating for brands and other folks that are trying to take action. And so, one of the things that I would like to say about Microsoft is, and I'm speaking with my BC hat on at the moment. But I'm also a member of the registry stakeholder group. And we're an accredited registrar.

So, we're in the CPH as well. And Microsoft has different organizations that combat cybercrime and digital crimes and botnets across the board. So, there's multiple aspects of interest when it comes to Microsoft, including trademark enforcement. When I spoke to my trademark teams at Microsoft and LinkedIn, and just asked them what their expectation was and what their

view was of the UDRP, which has been traditionally helpful and everything like that.

So, I don't want to sound pessimistic about that. But there was this sort of expectation of something's going to be better and different now that the gTLDs have their registry and registrar agreements updated to include some kind of compulsion to be a little bit more helpful. And I think that the feedback that I received internally was that they weren't seeing that uptick in helpfulness. And so, they're really interested in us being able to have this kind of dialogue. So, I could say more, but I think like I started off saying, it's pretty obvious and there's a lot of experts here. But if you had any questions for me, Reg?

REG LEVY

So, there's two things missing from this list from my perspective. In this case, it was indicated that a CDN was used. So, report it to the CDN as well. They are going to have more information about who is accessing it, how it's being used, and that sort of thing. I know they can also be difficult to get your hands on and figure out who they are and how to contact them. But if you need help with that, please let me know because I know people at some of these CDNs and they can give you those email addresses so that you can report these things.

COLE QUINN

Excellent. Thank you. The other thing I was going to say is that our corporate teams are vending a lot of this work out. And so, the

vendors, by the time that the information gets down to the vendor level, some of it gets lost in translation. So, being able to get real crisp with the TSG, with the method of procedure, like this is how we want to do it.

REG LEVY Sorry, what's TSG?

COLE QUINN Troubleshooting guide, sorry.

REG LEVY The technical stakeholder.

COLE QUINN A lot of, yeah, sorry, sorry. I out-acronymed myself. But most of the time that I was seeing the cases and the examples that they provided to me, they were going directly to the hosting providers and to the CDNs. And I had to clarify with them that we're actually just focusing on the registrars and registries for gTLDs at this point. But point well taken. It's a mix of tools in your tool bag, right?

REG LEVY So, the other thing that's missing from here, and it speaks to the UDRP point of yours, is the URS. Because if this is as obvious of a trademark issue as it seems to be from your end, because I don't know what the domain name is, and that's fine. Then it's, I believe the URS should be, was intended to be faster and cheaper than

UDRP. It may not get you the domain name. That may not be your end goal anyway. But it should take care of the issue of the content that you dispute.

You also said that you, your teams had not found that things were better or different post the amendments to our contracts. I would hope that they found it to be better and different for DNS Abuse. But we don't consider this to be that. And I know that that is also a point of contention. But I do see a queue. Oh, she put, dropped her hand. Do you want to? Oh, okay. Yeah. Okay.

OWEN SMIGELSKI Reg, was that your hand?

REG LEVY No, that was, yes, that was my hand.

OWEN SMIGELSKI Okay. Brian?

BRIAN CIMBOLIC Thanks, Owen. Hey, Cole. Brian Cimbolic, PIR. So, a couple of things. One, to Reg's point, that a specific trademark issue on its own is not included in the definition of DNS Abuse in the amendments. However, there's obviously this sort of Venn diagram. There is the intersection with phishing. If someone registers Microsoft Online dot whatever and has a credential gathering site there, that's obviously phishing. But if they have

Microsoft Online and have a foreign language casino site that is not trying to trick anyone into thinking they're on Microsoft, then that's obviously a trademark issue, not obviously a DNS Abuse issue. But when you are in that sort of shared area in the Venn diagram, especially as you're talking to registries and registrars, the one thing I would really encourage, and I'm happy to talk to anyone about this, is sort of changing your messaging as to when you're sending something to a registry or registrar.

We will get two, three-page, single-spaced demand letters saying the long history of the trademark, the prestige of the brand, and blah, blah, blah, blah, blah, blah. And I'm just reading it, reading it. And then also, the very last sentence is, also in Appendix B, because there's already an Appendix A for some reason, also in Appendix B, here's screenshots. It appears that this is a phishing site. And it's like, that's all we needed.

If you want to mention all the trademark stuff, sure, you can. And that might violate a registrar's terms of service. Independent, they may act independently depending on the registrar. But if you want to leverage the DNS Abuse amendments, it really does have to be specific to the phishing.

OWEN SMIGELSKI: Thanks. Just to reiterate, don't bury the lead. Start off with that and then give that additional context. Volker?

VOLKER GREIMANN

Yes, thank you. This looks like a response that we might have said not, because that is our default response when we cannot identify phishing or DNS Abuse. We tell the complainant that this is a brand issue, a trademark issue, a legal issue, that we are not equipped to decide for them, unless it's blatantly obvious. And then we will direct the complainant to resolve the matter directly with the registrant or the hosting provider through legal means or UDRP. However, that does not mean that this is the final answer.

If you can then come back to us and say, look, this is actually phishing because this and that and that, you haven't looked at this, we'll look at this again. If you are saying we cannot find the registrant or the registrant is somewhere where he cannot be reached by legal means and the hoster is somewhere else and we've tried to reach out, we will look at this again.

So, we're just saying we are the means of last resort. There are ways to deal with this directly, go there first. And if you have no success there, we'll look at this again. And obviously for urgent cases, that can happen very quickly.

REG LEVY

I'd also like to flag, I don't know what the domain in this case was or if it was also related to the trademark, but to the extent that it was telling us that it has active MX records or that it has a TXT record that directs to a Gmail account, that might be additional information that might be relevant toward the usage of this domain

in a spam scheme, in a phishing scheme, in a business email compromise scheme.

Again, I don't know if any of those things were true specifically for this example, but even if there isn't phishing that is identifiable on the site, it may be the case that active MX records will cause a registrar to take additional action. And Vivek, I see your hand.

VIVEK GOYAL: Simple question to everybody. When we are doing complaints, do registrars prefer an attachment of a PDF attachment or do we just dump all the information in the email body and that helps, makes it faster?

REG LEVY: Email body please. I love it when lawyers know how to use email. Email is a replacement for mail. Think of it as the envelope itself. So, put into the email what you want me to read. Do not put in the email, please see the attachment and read it. Obviously, we want screenshots and those need to be attached.

So, we do still need attachments, but those should be hopefully PNGs or JPEGs. Maybe it's a PDF with an embedded image, great, but put everything into that email because we have CRM systems, Customer Relationship Management Systems that don't do great with PDF attachments. So, as much information as you can put in the actual email is excellent.

OWEN SMIGELSKI

Before I go to Volker, just want to do a quick time check. We've gone through three out of 10 slides and we're halfway through. I still need to get to the CPH ones. I think we can probably squeeze ours into 10 minutes. Yeah, we can do five minutes maybe because they're pretty easy. I don't need to read them all to you, but I just want to make sure that we address your issues and concerns. But just keep that in mind. Volker, you're up.

VOLKER GREIMANN

Yes, further to what Greg was saying, attachments are also not searchable for us. So, if you have the information in the attachment, we will not be able to find that ticket again. Or if we are looking for parallels or patterns, then that domain name will not appear in that pattern simply because it's not searchable in the CRM system. So, it's good to have an attachment for additional information, but the basic information that we basically presented, that Graeme presented at the beginning, that is the essential information for the complaint should not be in an attachment.

REG LEVY

That information was in the last session.

CHRIS LEWIS-EVANS

And then, so in this case, the entity reporting reported it to the registry the day after. Next slide, please. And that was captured off of an automatic screenshot for the same site. It'd been updated, obviously, and now we're clearly phishing and the registry put it on server hold. So, that was the full course to show that process does.

And when there is clear there, that action taken. But sometimes people do stand-up sites to convince people and get traction. So, is there a place to act when there's clear and convincing evidence?

REG LEVY

Yes, this is clear and convincing and it is our place to act. If you have updated information for a previously submitted report, absolutely, please provide it. If this is the first image that we saw, we obviously wouldn't be here talking about it. And that's also why the registry took action. If you had sent the registry the exact information that you sent to the registrar, I doubt that any action would have been taken. Again, always happy to have more information, more data, please recheck.

CHRIS LEWIS-EVANS

Volker?

VOLKER GREIMANN

Just a small addendum. It's really hard to identify potential phishing domains. We get a lot of complaints about this domain name has been recently registered. It may be used for phishing in the future. It's currently parked. It might have MX records that may be used to send out phishing emails, but may also be just used to offer the domain name up for sale or whatever.

So, MX records themselves are not necessarily indicative of phishing. They might just be providing a clue. But any additional information that you have that shows that this is actually intended

for that is helpful. Because otherwise, if we cannot make that determination clearly and without doubt, it's very hard for us to take action.

MARIE PATTULLO: If we could have the next slide, please, and hand over to Philippe.

PHILIPPE FOUQUART: Thanks, Marie. So, this is, as we expect, adapted from a real case, which was reported, I think it was in November. There was an acknowledgement of receipt. So, the trick here is essentially that the first letter is changed from an I to an L, small k's. The website reproduces an older version of the original website. The contact us section of that website is intended to collect security information since that's the business of that company. The case was reported through the abuse email to no avail. And likewise, there was a request made to the hosting provider with that result.

OWEN SMIGELSKI: Volker, want to jump in?

VOLKER GREIMANN: Yes, sure. First, this is highly indicative of problematic because usually trademark abuse cases that misuse domain names are not homographs, but rather homoglyphs, but rather fat finger typos. So, that might be an indication. However, if you use the same email address, the same email to report it to the hoster and the registrar at the same time, maybe both parties saw that the other was

already alerted and thought, eh, they're already alerted, so they might take action. So, that might be a confusion.

So, please report in separate emails, not in bulk emails to everyone. Privacy Proxy may be indicative, but we have certain resources to register everything through privacy proxy because of the privacy concerns to registrants. So, that might not be anything worth reporting because it's simply something that the reseller does for all of their customers. So, that's not necessarily indicative. But if we are sent something like that, that would probably be something that we would have a higher view of potential abuse than something else.

REG LEVY

Yeah, and my answer would be quite similar to his. For you, use of a registrar's privacy service or of a third-party proxy provider might be evidence, but for us, it's typically not because as Volker indicated, we have relationships with a lot of these groups or they are us, right? So, we actually see the real data. This does, in fact, look like a trademark concern to me. Is there a phishing attempt? Are there active MX records? This is not, to me, very different from the prior example where you are seeing a significant trademark-related issue, but I am not seeing any active DNS Abuse. I see a Contact Us page. That's a hard one. Contact Us is requiring your name and email address.

That may, in fact, be sensitive data. Also, everybody's website has a Contact Us page. So, I don't think that I would necessarily see that as a phishing attempt. In addition to all of these other things,

there might be a nexus that would cause us to take action, but just on its face of this, I would say probably not.

VOLKER GREIMANN: Although the copying of the site might be something that we would probably consider as potential phishing.

UNKNOWN SPEAKER: Agree with Volker. I actually probably would have taken this down. That said, did you put your information in the contact form and see if they actually contacted you? Because that could have been, like I put my information in here, they reached out pretending to be the bank or whoever it was asking me for information.

If you've done that full process for a registrar and then documented it for them, I think that adds a lot of information as well because our agents aren't going to fill it out with their email and ask that someone, like no one's going to email or call Reg at Tucows back if she's the registrar for this, but they might do it for you. So, I actually recommend for this one, making it a slam dunk case, saying they are actually trying to reach out and pretend to be the bank through other means.

VOLKER GREIMANN: And maybe just one more addition because that is something that we also see a lot of. Some people abuse affiliate services or programs that the provider that is being copied here is providing and it's not a copy of the website, but rather forwarding, using the

domain to forward to the actual site of that provider using the affiliate link and therefore getting affiliated traffic, making advertisement, spamming for that site, driving people there to basically generate affiliate income and we would not see that as phishing either. And then we get the complaints that this is a copy and we see it's not a copy, it's actually the actual site that's forwarded to. So, yeah, difficult. Sometimes these cases are not as slam dunk as they appear.

REG LEVY

I would also say there's a, the registrar has been contacted repeatedly through the WHOIS Abuse email address. I know that our WHOIS Abuse email address provides an autoresponder that says, this is not a report, please go online and use our forms. So, it's entirely possible that your customer thinks that they have been regularly contacting the registrar and we have email logs saying that they got a response, an autoresponder every single time, that this wasn't how they should be reporting it to us. So, I just want to flag that, sorry, I should be speaking in this direction since you're the one who is presenting it. I just want to flag that for your customer's information.

PHILIPPE FOUQUART

Thanks, that's useful. I have to say that to your question, we didn't try that. That's a good idea. I should have made clear that this was reported by the affiliate that's in charge of the brands. So, that's

not the sort of things that they do, as you would expect, but we may try that.

UNKNOWN SPEAKER

Right, because then we get in a situation where they don't do that, well, we don't do that either. So, then someone has to figure out if they're actually doing malicious things with that information or not, and whose responsibility, if you want it taken down, I would take that upon themselves.

MARIE PATTULLO

And handing over to John from the IPC. Next slide, please.

JOHN MCELWAINE

Okay, so for both of mine, by the way, all the names and stuff like that, I ran through chat GPT to kind of come up with, hopefully, some creative names. Scarily enough, on the second one, I live in Charleston, South Carolina, and for some reason, it must have known where I lived, and it used my hometown as an example. But anyways, the first one I have here is for copyright infringement. In this case, the registrant is operating a website under Manga World Books using the domain name mangaworldbooks.com.

They're just blatantly violating copyright, selling hundreds of manga comic books for download without proper authorization from the copyright holders. Trade organization, Manga Rights Association, representing the interests of the publishers and creators, is helping its members out and discovered this

widespread copyright infringement. They sent a formal takedown letter to the hosting company, Webhost Pro, but nothing was, and they provided all the correct evidence, but nothing was taken as a result of that, no action was taken as a result of that request. Go to the next slide, please. So, the MRA then turns to the registrar for help. They note that the registrar's terms prohibit violating laws, including applicable federal, state, local government, or international laws, which copyright infringement would be one, and also prohibited copyright infringement.

So, they then send that same detailed request to Domain Secure highlighting the hosting company's failure to act. Of course, the registrant can't be uncovered, is completely hidden, and emphasizing that the operation of the website was violating the terms of use. What should Domain Secure, the registrar, do in this case?

REG LEVY Thank you, John. File a lawsuit. So, this, to me, seems to very clearly indicate a conflict of jurisdictions. You've got a registrar in India. You've got, I think, if I read this all correctly, and I'm going to guess that Manga World is based in Japan. And who knows where the hosting company is, right? So, if the hosting company is in the United States, maybe they can do a DMCA. If they're not in the United States, I know that they can't. But as you said at the top of the first slide on this, this is a clear copyright issue. This is content. This is not DNS Abuse.

There may be some registrars that are perfectly happy to deal with copyright, and there are other registrars that may not. That's going to be up to the registrar themselves. I will say that with regard to my terms of service, they are to protect me. They protect me from my registrants. They are not to protect a random third party. In fact, there is probably a clause in there. I hope there's a clause in there that specifically says that these terms of service are not intended to provide any rights to a third party. So, Mongo world quoting my terms of service at me is not going to get them anywhere and may, in fact, annoy me even more because they are very clearly trying to use what seems to me to be either a legal loophole or a profound misunderstanding of terms of service in order to get me to do something that they know I'm not going to do or they know that I'm not inclined to do, and that's the only reason that they're resorting to that.

So, in this case, I would strongly recommend some sort of a court order, some sort of a court order in a jurisdiction that one of the affected parties is going to obey. You also said at one point, which I don't think is specifically in here, that of course the registrant is not contactable or not findable. This to me is the perfect example of when to request who unmasked WHOIS data. This is an RDRS request. This is a TACO request. So, if you give me this, absolutely I'm going to tell you who the registrant is. Goes to them.

OWEN SMIGELSKI This is Owen Smigelski. And just a phrase I heard when I was at the UDRP panelist workshop a year or so ago, one of the UDRP

panelists said that the UDRP is not a domain name arbitration proceeding. It's a trademark claim. Domain name registrars are not IP rights arbitration tribunals. We lack the resources to be able to do that. And yes, I see there's a lot of things, there's frustrations.

When you're a big domain name registrar like Namecheap, you get a lot of people registering domain names that are similar to yours. And so, I sympathize with those concerns about IP issues, but it's not for the registrar to do that. We lack the ability to consider all the different, to adjudicate those things. And so, it's very difficult, especially when we're going to cancel a contract, basically, if we do suspend. So, that's what we do need the intervening courts who are more-better equipped to do that. Volker?

VOLKER GREIMANN

Just to add to that, copyright is not what we usually deal with because it happens somewhere else, not under the domain. The domain is not the problem. The problem is where the content is. Therefore, we need to be absolutely sure that this has been determined by higher authority as problematic on the legal aspect. So, we will not substitute our decision for a court decision and say, look, this is copyright infringement because we do not know everything that may be happening behind there. But maybe it's an old license that has expired.

Maybe they are perfectly legal to do that in the jurisdiction where they operate. But if you present us with a court order from a court in the jurisdiction that has some relevance to us, that we can respect, then even if it's not our own jurisdiction, we will take that

as potential evidence against a potential violation of our terms of conditions. And therefore, we might take action based on that.

So, do not expect us to determine whether something violates someone's copyright or not. But if you can provide a court decision that clearly demonstrates that, then that would be evidence that we can use. Catherine?

CATHERINE PALETTA

Thanks, I'll be quick because I think Owen and Volker made really good points. This is Catherine Paletta from Identity Digital. We also have a registrar called name.com. One of the things that we're talking about, these are big questions of fact that we're getting one side of. This is what courts are very good at determining, and we are not. It's not just that, but you can lie to me. You get in big trouble if you lie to a court, right, at least in the United States.

So, not that you guys would lie to me, but that a malicious actor that doesn't like manga or doesn't like the specific manga that's up there that could be perfectly legitimate, right, might say these are all my copyrights and generate some documentation that seems to say that. And we don't have a way to, we're not set up to adjudicate that. And certainly, we don't have time is a big thing. I need things I can look at, determine, yes, this is within my box.

This is, we talked about phishing. I'm looking for these two things. I can see that, I can see that, great, phishing down. My staff doesn't have time to be adjudicating these types of things because we're trying to get to your next report of phishing or malware or

something so we can take that down. And so, I think that's also a piece to this as well. Thanks.

JOHN MCELWAINE

So, let's move on to the next slide. I think here, there's no other questions. Okay, so this next one is a bit more edgy. So, this is unregistered trademark with fraud going on. And this is the one where, again, I didn't put in where I was living, but the background of this is Charleston's Traveler's Haven is a small retail store located in the airport there in Charleston. And they sell all sorts of apparel, food, gifts, including liquor.

It's a popular store there, has significant sales figures, the type of stuff we put in a letter that would annoy the registrars. So, the owner of the store recently discovered that the domain name was, that a domain name identical to her store's name was registered, Charleston Traveler's Haven. It's registered, but to an unknown party. Again, we don't know who is owning it. And the domain name owner is operating a fake website that purports to sell liquor, leading to confusion. What's going on is she's receiving misdirected phone calls, unhappy customers, because the person that is operating that website is scamming people, taking their money and not delivering the liquor that they ordered.

And she's getting all sorts of negative Google reviews left as a result of this. You can go to the next slide. Again, the terms of use of the registrar would not allow that type of behavior. Demand letters sent to the abuse at the registrar named Nephew, explaining that

she had not registered the trademark, but had significant common law trademark rights, meaning unregistered trademark rights.

Provided all the evidence that we would think that the registrar would want to see a screenshot, an affidavit, and screenshots of the bad reviews alleging that people have been scammed. So, let's see. We assert that it violates the UDRP, national law, cybersquatting, et cetera. Fraud is being run. What should the registrar do in this case?

VOLKER GREIMANN Well, first of all, this seems like a slam dunk case for UDRP and also a police report. Standard fraud is very hard for us to differentiate from a site that might've been legally set up and then they split up an argument or there have been cases where such sites have been legitimate in what we have seen in reports in the past because of two parties no longer agreeing on how they split up their business or something like that. It seems like the report is trying to put the registrar in the position of a court and require us or request us to make certain assumptions that we might not be able to make.

So, yes, this could be fraud, might not be. Have you tried filing it with the police report? Have you tried legal action against the registrant? If you haven't, there's no way to deal with that. Provide some information to that and we'll look at that again.

OWEN SMIGELSKI I'm sorry. Catherine?

CATHERINE PALETTA

Thanks. I was going to point to, on the last slide, you kind of categorized this as unregistered trademark/fraud. Fraud is not DNS Abuse, right? We know what capital DNS, capital A DNS Abuse is. We know what the amendments say. But this looks like something you could get to me via phishing. Are they impersonating her website? Are they collecting user information? It sounds like they are. If you're ordering, you're ordering alcohol, you're probably somehow proving that you're old enough to order it, all this kind of stuff. Get me a phishing complaint.

I don't need to see your registered trademark in order to be able to know that someone's impersonating someone else and is collecting sensitive information. And so, to me, it doesn't really matter if it's a registered trademark or not. What matters is that you've ticked those two boxes and then it's phishing and we can take it down. Thanks.

OWEN SMIGELSKI

Chris?

CHRIS LEWIS-EVANS

Yeah, thanks. Chris Lewis for the record. So, Catherine, just on that point, so I'm going to hop back to my previous law enforcement. A lot of the times this sort of size of store doesn't have a website. So, what happens if a phishing complaint went in for this and they said, we don't have a website, but they are phishing our customers?

CATHERINE PALETTA

Speaking not on behalf of all anyone, any of the Contracted Parties, that's a lot harder. You're exactly right. Because like, I don't know how believable it is that this is someone pretending to be you if I don't know what they're pretending, right? We saw an example where they had copied the entire website was exactly the same except the contact us form, right? That makes it way clearer that they are impersonating you, right? I think that's a lot harder. I defer to my experts on my abuse desk on what they would do because I don't sit on that. But Graeme's got his hand up and he's maybe going to save me.

GRAEME BUNTON

Save is a strong word. Graeme Bunton from the NetBeacon Institute. Again, I think pulling up a little bit to see how this can be an example. I like to use, and I don't know that everybody adopts this language, but I think it's maybe useful, of deception of identity versus deception of function. Registrars are often able, usually most of the time, able to determine if a website is engaged in that deception of identity. Is it that actual brand? Yes, or no? And they can tell.

This case, I think, is talking about a deception of function. Is that a real store or not? And then they don't have access to whether that's the right website or not for that entity because that entity doesn't have an actual web presence. And so, I don't think they have the ability in this case, maybe, to do that verification on the deception of identity. And then they just can't be the arbiter of that deception

of function. Are they actually selling goods or not? And so, I think this is in a tough spot.

OWEN SMIGELSKI: All right, I think we're going to go to Reg now in the next slide because I think it's CPH, which we can kind of go through at a very high level.

REG LEVY: So, we're going to blitz through this in the next four minutes. So, 2.1 here, actually, you just presented to us a bunch of the cases that we would have done for you, examples of cases where there is no phishing, but you guys sure are convinced that there's something going wrong. I'm not arguing that there's not something going wrong, only that it's not DNS Abuse.

We've got example one on the next slide is basically exactly what you have previously indicated to us. It's just in a different format. If you could skip actually to 2.2 because we're going through these real fast, everybody's going to get these slides. You can read them. This one I'm going to turn back to Owen because it is a very unique use case.

OWEN SMIGELSKI: Yes, we literally just received this within the last week. It was asking us to remove this person's, they had a DMCA request, which they also sent to our CSAM address for some reason, claiming rights in these names. The names were a little more unique than what I

really put in there. But when you put in the person's name to this image generation website, which would do AI questionable stuff, I don't know, it wasn't always porn, it would return search results, not of Susan Professor, but just random designed images.

If I put in George Washington, it would do the same thing. But this person sent five or six complaints to us and they're a cyber law professor somewhere. So, we do get very intelligent people who put in really crazy complaints. So, this is kind of the noise that we have to get through, which is we're moving on to this and then yours. And so, there's a lot of stuff going on.

REG LEVY

Thank you. And if you go forward a couple slides to 2.3, yes, and the next one. So, I'm just going to briefly say 2.4 is a copyright complaint. So, again, the same as what you guys have presented to us as that we are presenting back to you as this is not DNS Abuse. Crypto scam allegations. I have had two competing domain names registered to my registrar, each one claiming to be the correct version of whatever meme coin they were and claiming that the other was phishing against them.

And part of me just wants to shut down anything that is cryptocurrency related because it's all a scam. I am not yet allowed to do that as far as I know, but this is a thing that we see constantly. We have no ability to make a determination about whether or not your meme coin is the right version, your customer's meme coin is

the right version and some other cryptocurrency online is the one that's phishing. And that's it. So, we got one minute, Owen.

OWEN SMIGELSKI Actually, I think we have more slides.

REG LEVY No? Yeah, we have more slides, but this one is the same as the manga.

OWEN SMIGELSKI Yeah. But then if just keep going, because I think there was kind of like a catch all at the end, not this one. One more, there we go. And these, yeah, the miscellaneous concerns, just check these out because these have some other high-level things that weren't necessarily exact complaints, such as when we receive a abuse complaint, the domain name is already suspended. You know, that kind of wastes the time because the DNS Abuse is no' there anymore. So, just take a look. These are some more feedback there.

So, I'll close here. If there's any questions with our slides or anything like that, please do reach out to us afterwards. Again, thank you to everybody in the CSG for trying to get a little bit better of an understanding. I think this was very helpful to kind of talk through it. I think we need more time and maybe some more examples, which we can possibly think about doing this in the future, because it's better than us talking past each other and

	trying to argue about it, but actually getting down and seeing these examples and having a very wide number of different types of registrars give feedback about why we did or did not action that, and sometimes the registry as well too. Sure, go for it.
UNKNOWN SPEAKER	Just to the first point, Google does have an intake form that you can say, please de-index this. So, don't go to a registrar, go right to Google for that one.
OWEN SMIGELSKI	Thank you. Mason?
MASON COLE	Thanks, everybody. Very helpful session. We appreciate it. Thanks, Owen. Thanks. Appreciate it.
SUE SCHULER	We can end the recording.

[END OF TRANSCRIPTION]