
ICANN75 | Prep Week – Contractual Compliance Update
Wednesday, September 07, 2022 - 02:00 to 03:00 KUL

MEHDI KURDMISTO: Thanks. Start the recording, by the way, if we haven't.

JAMIE HEDLUND: Thanks, Mehdi. Thank you all. Welcome to Contractual Compliance update presented as part of ICANN75 Prep Week. I am Jamie Hedlund, and I'm very proud to lead ICANN's Compliance team.

Today's presentation will generally cover the period of June of last year through May of this year. We will begin with a review of the ongoing registry operators audit to be presented by Yan Agranonik who heads our audit team. We will then move to an update of three of the most important areas for enforcement: third party access to non-public registration data to be presented by Amanda Rose who is our Compliance lead in several areas, including Registration Data Accuracy and Temp Spec-related matters, followed by DNS abuse, UDRP enforcement actions to be presented by Leticia Castillo who is the director in Contractual Compliance. And then finally, Jonathan Denison, JD, who is also a director in Compliance, will give an overview of our team's efforts to do education awareness. Next slide, please.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

So, a quick refresher on the role of Contractual Compliance. We ensure that gTLD registries and registrars implement the community’s consensus policies that are included in our agreements with contracted parties. We accomplish our mission through enforcement actions arising from external complaints, monitoring, and audits. We also actively pursue outreach activities to raise awareness of the obligations arising under agreements with the contracted parties.

Thank you again for attending today’s webinar. Yan Agranonik will now discuss the ongoing registry audit. Yan?

YAN AGRANONIK:

Hello, everyone. Actually, it’s not ongoing. It’s just being wrapped up. So in April of this year, ICANN Compliance launched a new audit round to test and validate registry operators, compliance with the Registry Agreement. It was a full-scale audit, meaning all Registry Agreement provisions were in scope. Unlike, for example, a previous limited scope audit which targeted specific selected obligations. So back in April, we published a blog where we announced the start of an audit, described its scope, described auditee selection criteria, which you can see on the slide. I’m not going to read it. You can see criteria right there.

By the end of May, we collected all the data and responses from auditees that we needed. With the help of our vendor, which is KPMG, we have reviewed over 3000 documents collected in eight different languages received from auditees located in 14 different countries. We also reviewed data received from Data Escrow Agents that service these registries, as well as from Trademark Clearinghouse. We also had access to data that registry operators periodically submit to ICANN.

At the completion of an audit phase, which was in July, ICANN issued initial non-public individual audit reports that we sent to each auditee indicating what initial findings, if any, were identified as a result of an audit. We asked auditees to address those initial findings.

Talking about results on a high level, I can say that approximately 10% of auditees received so-called clean audit reports with no initial findings whatsoever. The rest had one or more findings. Findings are very different in nature and difficulty to remediate, generally speaking. For example, it could be in the instance that a mandatory information is missing on the registry website, which is relatively easy to fix. Some other findings may require more time and efforts to address.

Approximately half of the registries were able to fully resolve their findings before the audit wrap-up, which took place at the end of August. The others explained how are they going to

resolve the findings and how much time would it take. Some of the time estimates were very few, were a little unreasonable, and we had to come up with a mutually agreeable timeframe. These registries that are currently working on remediations, they did not fail the audit. They provided a reasonable and specific estimated time for completion. And again, some of the findings do require some time to complete. ICANN will confirm the remediation plans that have been implemented. We will retest the timeframe they indicated.

So the audit was completed, like I said, by the end of August. The audit report currently goes through final internal review. As soon as this is done, it will be published. The link that you have there on the slide, it does not go to that report yet because it's not published yet. It goes to information about the audit program itself and the prior reports. I will gladly respond to questions at the end of this presentation.

AMANDA ROSE:

This is Amanda Rose. I can take the next slide. I'm going to discuss the disclosure of non-public registration data or registration data that's been redacted in the public data directory. This is currently enforced through the Interim Policy for gTLD Registration Data but that requires registrars to continue to implement measures consistent with the Temporary Specification for gTLD Registration Data which has the current

requirement, which is here on the slide, requiring contracted parties to provide reasonable access to that redacted registration data. And where applicable, the requirement to perform a balancing test, which essentially requires that they balance the alleged interest of the requestor with the fundamental rights and freedoms of the data subject.

So one thing that is coming up with the Interim Policy is we're currently in Phase 1. The next step would be Phase 2 and that has to do with when the Registration Data Policy will be published. And Phase 2 enables contracted parties to implement either the Temporary Specification or to begin implementation of the Registration Data Policy. This will replace the legit or the reasonable access requirement under the Temporary Specification with new requirements, and those are currently available in public comment.

So that's the phase we're in. That's a 68-day period. So I invite everyone to tune in. There'll be a session at ICANN75 relating to that, if you have any questions on the next steps there. But as far as the Jun 21 through May 22 data, we have that available on the slide and shows that we've received 121 complaints during that rolling year period. Majority of these, you'll see are from intellectual property (IP) lawyers, along with 23%, which is the catch-all of the remaining, and 8% LEA government entities or data protection authorities. 81 of these were closed as out of

scope. To clarify, there's a few main things we see as out of scope. A large majority of those are situations where it's a proxy service. So the actual registrant is the proxy service itself, and the full registration data is required to be displayed in the public registration data directories. So there isn't an issue of disclosure as it's all publicly available. So that's covered outside of the scope of third party requests under the Temporary Specification.

Another one we see frequently is that the data is actually there publicly available in the directory or WHOIS. Then finally, a lot of them we get our just failure to respond to requests for evidence to support the complaint, such as evidence that the data was requested from the contracted party. One more actually requests for historical registration data that might fall outside the scope of third party requests.

Now, of those, you can see that we did initiate 38 investigations with the contracted parties involved, and then 42 have been closed during that same time period. So just to explain that does include some that were initiated prior to the start of the metrics that we snapshot in that year period, which explains why there's more closed than initiated.

Finally, four remediation plans were completed by registrars. To clarify, that generally involves ensuring they have a policy in place to comply with the requirement within the Temporary Specification to provide reasonable access. So if, for example,

there's a blanket denial policy or failure to individually review requests that come in, then remediation might be required.

Finally, we have full metrics available on our dashboard. It has all the breakdown of the different areas of enforcement under the Temporary Specification, including third party access. With those, we have begun to publish additional details in February that explain was the data provided, was the request denied. Or sometimes, in some cases, additional evidence is needed or requested and the request itself is deemed incomplete. So that is available. We will include that in our snapshot once we have a full picture of that for the full calendar year. But you can find that at the link there. With that, I believe that wraps up my slide and I can turn it over to Leticia.

LETICIA CASTILLO-SOJO: Thanks, Amanda. Hi, everyone. My name is Leticia Castillo and I am going to talk about the enforcement of UDRP and abuse obligations, as well as the formal enforcement notices that we have issued since June 2021.

Let's start with UDRP. UDRP stands for the Uniform Domain Name Dispute Resolution Policy, which is a consensus policy that all registrars must comply with as a condition of their accreditation with ICANN. If a trademark holder believes a domain name registered by someone else is infringing on the

rights, he or she may choose to initiate a UDRP proceeding with an ICANN-approved UDRP provider. The procedure is administered by a UDRP providers panel. And a trademark holder or UDRP complainant, if he or she prevails, gets to dispute registration either cancelled or transferred to them dependent on what remedy of this to the complainant selected when starting the proceedings with the provider.

So, the UDRP is the policy itself. It says the scope of the relief and the basis for the proceedings. And then we have the UDRP rules, which provide the baseline procedural requirements that must be followed in a UDRP proceeding such as the obligation to lock the domain so it does not get transferred in the middle of the proceeding, notifying the respondent, time for filing a response, etc. At the same time, its provider also maintains its own set of supplemental rules that cover other topics such as fees or word and pitch limits, etc.

So, we enforce the UDRP itself, we enforce the UDRP rules, and all other requirements that relate to UDRP across all ICANN policies and agreements and specification. For example, Appendix E of the Temporary Specification for gTLD Registration Data, which is in effect pursuant to the Interim Registration Data Policy for gTLDs, it contains certain requirements where the personal data associated with the domain is redacted, or the Transfer Policy which prohibits a registrar from allowing a

transfer of a domain name that is subject to a UDRP proceeding. We enforce all of these litigations. This slide shows some metrics related to that enforcement. From June 2021 through May 2022, we received 126 new UDRP complaints. Most of those were submitted by UDRP providers, followed by self-identified UDRP complainants, and third place for registrants.

The top reason selected at submission was the registrar’s failure to timely lock domain and reply to the provider’s verification request. The UDRP rules explained that upon receiving a complaint, the provider sends a request to the sponsoring registrar to lock the domain to provide data associated with it. The registrar must do this within two business days according to the rules. When this does not happen, the providers can submit a complaint to us and we enforce the requirements with the sponsoring registrar.

The second reason for submitting a complaint to us during this period was failure to implement a decision. The provider rendered a decision which the registrar must implement 10 days after being notified of it unless there’s evidence of a lawsuit initiated by the respondent within the appropriate jurisdiction during those 10 days. When this does not happen, the decision is not implemented. There’s no apparent lawsuit initiated, a complaint can be submitted to us. We also enforce the relevant remediation with the registrar.

So you see on the slide how, during this period, we started 81 UDRP cases with registrars and resolved 98 that had been initiated with registrars. Most of the resolved cases had been submitted by UDRP providers and resolved after the domains were locked. We're talking about that one before. And we obtained evidence that the information requested from the registrar had been provided to the UDRP provider. You can see there that nine of those related to Appendix E of the Temporary Specification data was redacted.

Regarding those submitted by UDRP complainant, most were resolved after the registrar demonstrated compliance, which mostly means that the registrar implemented the decision after being contacted by us. But also we have situations where the registrar provided us with evidence of the lawsuit that had been initiated and supported that lack of implementation of this issue.

We did issue two formal breach notices related to UDRP obligations during this period, both related to failure to implement a decision. One of them escalated to suspension of the registrar's accreditation for four months. Decisions were ultimately implemented. Both breaches work here.

We also have three additional cases that we're about to result in breach notices that were clear right before we send them, two of them related to provider's request and one had to do with the

obligation to allow the UDRP complainant to renew or restore a domain the had expired through the UDRP proceedings, and the registrar was not responding to the complainant in this regard.

We also had 16 remediation plans presented and completed by registrars during this period that relate to UDRP. This generally stems from a complaint and we detect some errors related to the registrar’s operation. It could be technical, it could be human, that may continue to negatively impact UDRP-related matters if they’re not fully addressed. So we ask the registrar, in addition to addressing the complaint at hand, like implement a decision or locking the domain, they provide us with a plan to address the root cause, so it does not continue to affect other cases in the future. This is plan may include depending on the cost of the failure, whitelisting all UDRP providers’ e-mails, hiring additional staff, providing additional training staff, addressing technical glitches that prevented the correct login of the domain, etc. So we get the plans, we close the relevant cases once they’re implemented, and we track and monitor. Next slide, please. Thanks.

So here we have the enforcement of registrars’ obligations related to DNS abuse, which are in Section 3.18 of the Registrar Accreditation Agreement, and are to take reasonable and prompt steps to investigate and respond to these reports that are submitted by any user. There are also requirements related

to review reports within 24 hours and where they are filed by law enforcement and other authorities within the registrar's jurisdiction. The obligation to display abuse contact and a description of the registrars abuse procedures, so users know how to submit abuse reports to the registrar and how those reports will be handled, and the obligation to maintain records related to the abuse reports and provide them to ICANN upon notice.

When we investigated these abuse complaints, in general we request an explanation and supporting records concerning how the registrar addressed the specific abuse report, as it is required by the RAA and in accordance with the registrars on domain name use and abuse policies. We do request as much information as possible, as much [inaudible] as needed to ensure that this was done, and then we have evidence of it. We do not have, however, contractual authority to require the registrar to take a specific action on the domain name such as suspend it or remove certain content in response to an abuse report, because those are not actions that are specifically mandated by the RAA, the registrar [inaudible] minutes I mentioned before.

Here are some metrics concerning our enforcement of these obligations from June 2021 through May 2022. We received 3461 new abuse complaints and we sent over 719 abuse notifications

to registrars requesting the evidence, the explanation, and all the details that I mentioned before. We closed 604 cases with the registrars because they demonstrated haven't taken steps to investigate and respond to the abuse report.

Approximately 40% of the cases, the registrar suspended the domain name or domain names that were subject to the complaint. We issued two formal breach notices to registrars who failed to demonstrate compliance with their abuse obligations. We're presented with two remediation plans from registrars. Again, regarding this remediation, we asked the registrar to provide them because we detected an issue that needed to be addressed to prevent the recurrence of the non-compliance beyond individual complaints.

We closed 3601 complaints without initiating an investigation with the registrar. Approximately 70% of the cases because there was no evidence that the complainant ever attempted to report the matter to the sponsoring registrar. One of the first contractual requirements that we were talking about before is to investigate and respond to these reports that the registrar receives. So there must be an abuse report filed with the registrar first to trigger the requirement. However, many complainants misunderstand our role and our authority, and they believe they can report the activity to us directly. They ask us to delete domain names. They sometimes ask us to transfer

the domains to another registrant. And for these cases, we provide an explanation of our role and any other information that can be helpful for the complainant, for example, how to find the sponsoring registrar, where to look for its abuse contact. If they have additional questions, we do our best to address them and provide them with any assistance we can within the bounds of their agreements. But those are closed without contacting the registrar.

In 10% of the cases, the domain name was already suspended by the time we were reviewing the complaint. There are other small percentages, like those that are involved ccTLDs or the complaints, for example. I think this is all for this slide. Can we please go to the next one? Thank you.

So we talked a little bit about disclosure of gTLD registration data, UDRP and abuse. These are just three complaint tests for which we enforce all obligations within the relevant agreement policy specification. Now, for context, during this period that we're talking about, we received almost 14,000 new complaints across all complaint types, which is three. Across all complaint types, most cases were closed within the informal resolution stage or process which generally comprises three notifications and two phone calls through which we communicate to the contracted party what's necessary to demonstrate compliance. For the most part, contracted parties do timely provide evidence

of compliance at this point and the cases are closed. But if the informal resolution process is exhausted, we escalate the matter to the formal resolution stage where a notice of breach is issued to the contractor party. This notice is published on our website. It states the specific areas of non-compliance and what needs to be done to cure and by when. Failure to fully and timely address these notices results in a suspension or termination of the accreditation for registrars or the initiation of termination proceedings for registries.

Now, from June 2021 to date, we have issued—you see there 11 breach notices that included failures to comply with obligations such as providing WHOIS service, escrowing data, implementing UDRP decisions, or investigating and responding to these reports. Three escalated to suspension of the registrar’s accreditation for three months. One of them was actually extended by one additional month later on. And we terminated six registrars for failure to procure breach notices.

At the bottom of this slide, you have a link to our Enforcement page, which would have all the notices in case you want to read them. As we did say before, we’re going to publish this slide as well. I think this is all from me. I am going to hand it over to Jonathan Denison for the outreach update. Thank you.

JONATHAN DENISON: Thank you. This one will actually be pretty quick so we can get to some of your questions there about UDRP and abuse. But basically, this is regarding outreach activities conducted by Compliance. This tends to include various methods of outreach. Sometimes we have organized activities where we're part of a broader group such as that first bullet there. In June, there was a virtual session for Turkish registrars organized by Global Stakeholder Engagement and Global Domains and Strategy teams. The session was delivered in Turkish language and Compliance covered topics such as abuse, UDRP, and data escrow obligations. Then other times there's outreach that's conducted just from our day-to-day work through various cases that we're processing. Sometimes if there are issues that we think might be best addressed over a phone call, we could always send a request to the contracted parties, or contracted parties can request them to our cases.

Since the last ICANN meeting, we've conducted numerous calls under both conditions to clarify contractual obligations and the compliance process. The calls are often conducted in different languages. And even though the step might stem from one category of complaints or complaints, many times they actually cover various obligations that might intersect within a particular type of issue such as RDDS display, UDRP, or abuse obligations.

So, that's pretty much it for outreach. I think that's it for our slides. Leticia, did you want to answer some of these in person?

LETICIA CASTILLO-SOJO: Sure. Okay. So the first question is regarding UDRP. "If 81 new investigations were launched but 126 complaints submitted, what was the outcome of the other 45?"

Thanks for your question. We were talking about the events occurring within June 2021 through May 2022. So it is not 126 minus 81. Let me explain. A complaint may be received in May 2022. So it counts toward complaint received and the investigation for this specific complaint is initiated in June 2022. With this in mind, to answer your question, some of these investigations related to these new complaints were initiated—after the time period that we were talking about, some of them were closed because they were invalid complaints. This happens across all complaint types, kind of like I was talking about regarding abuse. We close them, we provide the explanation that can be helpful for the complainant, but we do not initiate a case with the registrar. I hope that answers the question. JD, do you want me to go to the next one?

JONATHAN DENISON: Yeah, go for it. These look like they're all on your slides. So just let me know.

LETICIA CASTILLO-SOJO: “On abuse, are the two formal breach notices the same registrars as the remediation plans? Received in the form of breach notices, did the registrar then act to propose remediation?”

So for these specific cases, one of them related to the breach. So there was one remediation plan that was provided in response to the breach notice, again, within this period. But also to answer your question is generally when we go to a breach notice, we will request remediation plan as well as the matter had to escalate to the formal enforcement stage of our process. I think next one is very clear.

JONATHAN DENISON: Yeah. If you could just read the question a little slower, that’d be great.

LETICIA CASTILLO-SOJO: Okay.

JONATHAN DENISON: Thanks.

LETICIA CASTILLO-SOJO: “Could you please speak to the timeliness of resolving abuse complaints? In other words, how long did it take to resolve the issues in the 719 cases where ICANN Compliance elected to notify the registrar? How long did the 604 cases take to get resolved on average?”

So this is not an easy question. Each case can be different. It depends on the complaint. It depends on the details of the complaint. Sometimes we do have to do outreaches with the registrars, like JD’s going to mention in a minute. So it depends. Some cases that I have seen were resolved within a matter of a couple of days. We send an inquiry and the registrar will reply right away. Some others may take a couple of weeks, three weeks, it depends. And those that escalate to formal enforcement, because they normally go through notice to notice phone calls, they may take a little bit longer. That said, JD, did I miss any question?

JONATHAN DENISON: it looks like all I can see. And Amanda put a response in the chat question. So I guess what we can do is see if there’s any last-minute questions for us. I’ll leave it to Jamie and Mehdi.

JAMIE HEDLUND: So barring any further questions, thank you all for listening. Our door is always open. If you have any concerns or thoughts or

recommendations or constructive criticism, please share them with us, to any of us individually or to the compliance@icann.org e-mail address. I think I have that right. I look forward to seeing many of you in Kuala Lumpur. Thank you.

MEHDI KURDMISTO: Before we close out, we did receive one last question.

LETICIA CASTILLO-SOJO: Let me see the question. “Did you receive any complaints about UDRP providers? Are they dealt with by your team?”

We do not normally disclose the absolute details of all the details of the complaints that we receive unless they go to the formal enforcement stage of our process.

JAMIE HEDLUND: Leticia, I think she’s actually asking about the providers themselves.

LETICIA CASTILLO-SOJO: I think it’s about the UDRP providers. Correct, Susan?

JONATHAN DENISON: “Yes” in the chat.

LETICIA CASTILLO-SOJO: So yeah, that was the answer to that unless, Jamie, you wanted to add something?

JAMIE HEDLUND: No, that's it. Thank you.

LETICIA CASTILLO-SOJO: “Does the Compliance website advise people not to submit a report if they have not submitted to the registrar on a DNS abuse?”

Thanks for your question. We do have a brief explanation of the requirements at the beginning of each form. So it does, the form itself, explains that an abuse report must have been submitted to the registrar. In addition, the form itself provides a link to the WHOIS service lookup so that the reporter can write their check who the registrar is and some information how to find the abuse contact details.

JAMIE HEDLUND: Just to clarify, so the obligation under the Registrar Accreditation Agreement is for a registrar to receive abuse reports, and then to investigate and respond. So unless the registrar has received a report of abuse and the concern is that they did not act on it, there's nothing we can do. Obviously, reporting to the registrar about a potential abuse is important,

and we will follow up on complaints against registrars who appear not to have fulfilled their obligations to investigate and respond. Thanks.

MEHDI KURDMISTO: Thanks, everyone. It looks like all the questions have been answered. Thank you to the speakers. Thank you to the participants.

LETICIA CASTILLO-SOJO: Mehdi, I think there's a question in the chat.

MEHDI KURDMISTO: Sorry.

YAN AGRANONIK: I think it's a question to me. "What penalties are inflicted to registrars in case violations found during RA Compliance audit?"

The procedure is, first you deliver the findings to registrar. And essentially, you tell that—by you meaning us—Compliance delivers the message to registrar and saying, "Here's what we found. Please confirm that what we found is indeed the case because it maybe we didn't understand the response or maybe we're reading something incorrectly." So when the finding is

confirmed, the registrar is asked to remediate, essentially. If remediation is done in a timely manner, there are no penalties.

The only penalties may show up if registrar ignores the message, basically. So we deliver the message and there is no response, so there will be a second notice, third notice, and if they continue to ignore our messages, then it goes to enforcement and there will be a breach. That is the only penalty I can think of, or registrars refusing to address the issue. But this has never happened. What did happen is that registrar, for some reason, either delaying response or not being responsive at all. I hope I answered the question.

JONATHAN DENISON: Yan, it looks like you got another one popping in there. “Do Compliance audits of gTLDs include eligibility requirements?”

YAN AGRANONIK: Yeah, I see the question. No, it did not.

JONATHAN DENISON: Okay.

MEHDI KURDMISTO: Any last messages, comments, questions? We received another question. “Are complaints re non-compliance with eligibility requirements accepted?”

JONATHAN DENISON: Could you perhaps elaborate, Yan?

YAN AGRANONIK: By eligibility requirements, are you referring to a registrant being eligible to registrar a domain in a restricted TLD? Okay. So the complaint would be that someone is complaining that the registrant was able to register a domain without going through certain eligibility verification. Okay. That’s question to Leticia, I suppose.

LETICIA CASTILLO-SOJO: Actually, I believe it’s a question for JD for the registry area.

YAN AGRANONIK: Before JD responds, I have to go back and correct my statement. I didn’t understand, I guess, first, your question about eligibility. Yes, we do verify the eligibility procedures. Verification procedures do exist in the restricted TLDs. But as for complaints, that’s JD’s question.

JONATHAN DENISON: Yes, sorry. Yan, can you just reiterate or reread the question?

YAN AGRANONIK: The question is, “Do we accept complaints regarding verification of eligibility in restricted TLDs?” For example, if I understand the question correctly, if you have restricted TLD where the procedure is that TLD or registrars supposed to verify certain eligibility criteria before registration and they do not do that, do we accept this type of complaints, if there are any?

JONATHAN DENISON: Obviously, we accept all complaints. But I think it’s one of those where we would have to look into if there are any specific cases off the top of my head. It’s not something that I can imagine occurring often. So yeah, if we add more details, anyone can submit a complaint and let us determine whether or not it’s something we can address.

MEHDI KURDMISTO: There’s no open questions. No new messages in the chat. I’ll give a couple of moments for any last comments.

Okay. I believe it’s safe to say we have completed this session for today. Thank you everyone that participated. Thanks for all the questions. Thank you to the panel. Again, you can send any

questions you might think of after the fact at
compliance@icann.org.

JAMIE HEDLUND: Thank you all.

JONATHAN DENISON: Thank you.

LETICIA CASTILLO-SOJO: Thanks, everyone.

[END OF TRANSCRIPTION]