ICANN Contractual Compliance Response to Questions from the GNSO Council DNS Abuse Small Team

Jamie Hedlund
SVP, Contractual Compliance and U.S. Government Engagement
2 May 2022

Introduction

This document attempts to respond to the following written questions posed to ICANN Contractual Compliance (ICANN Compliance) by the GNSO Council DNS Abuse Small Team:

1. Can you please provide an overview of the current requirements that Contractual Compliance enforces in relation to DNS abuse (e.g., relevant provisions of the Registry Agreement and Registrar Accreditation Agreement)?
2. Can you describe how the enforcement of these provisions practically takes place from a procedural standpoint, including if there are any unique process elements for DNS abuse related complaints? In addition, besides responding to submitted complaints and performing audits, are there any other mechanisms by which Contractual Compliance identifies actionable information to investigate DNS abuse related complaints?
3. Do you have any metrics and/or trends that provide further insight into the complaints that are investigated by Contractual Compliance in relation to DNS abuse?
4. What are the factors that Contractual Compliance takes into account when reviewing a DNS abuse related complaint? Are there factors, whether in whole or in part, which are applied across the board ('mandatory') as opposed to on a case-by-case basis ('discretionary')? Are there any challenges in determining whether a Contracted Party is failing to comply with their contractual obligations regarding DNS abuse? If so, what would assist you in making such a determination?
5. If you have determined a Contracted Party is failing to comply with their contractual obligations regarding DNS abuse, are there any challenges in effectively remediating the compliance issue? If so, what would assist you to ensure effective remediation?

Question 1: Can you please provide an overview of the current requirements that Contractual Compliance enforces in relation to DNS abuse (e.g., relevant provisions of the Registry Agreement and Registrar Accreditation Agreement)?

ICANN Compliance enforces the contractual obligations set forth in ICANN's policies and agreements, including the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA). Examples of the abuse-related provisions enforced by ICANN Compliance include RA Specification 6 4.1, Specification 11 3(a) and 3(b), as well as Section 3.18 of the RAA.

- **RA Specification 6, Section 4.1**. Registry operators shall provide to ICANN and publish on their websites their accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the top-level domain (TLD) and provide ICANN with prompt notice of any changes to such contact details.

- **RA Specification 11, Section 3(a)**. Registry operators have an obligation to include a provision in their agreement with registrars, for registrars' agreements with registrants to prohibit registrants from engaging in certain activities, and requiring consequences for the registrants for such activities, including suspension of the domain name.

- **RA Specification 11, Section 3(b)**. Registry operators are required to periodically conduct a technical analysis to assess whether domains in their gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. In addition, registry operators are required to maintain statistical reports on the number of

security threats identified, including the actions taken as a result of the periodic security checks for the term of the Agreement, and to provide copies of these reports to ICANN upon request.

- **RAA Section 3.18**. Registrars are required to:
  - Take reasonable and prompt steps to investigate and respond appropriately to abuse reports;
  - Review well-founded reports of Illegal Activity (as defined in the RAA) that are submitted by law enforcement, consumer protection, quasi-governmental or other similar authorities within the registrar's jurisdiction; and
  - Publicly display abuse contact information and abuse report handling procedures for users to know how to submit abuse reports to the registrar and how those reports would be addressed.

Similarly, ICANN Compliance enforces other contractual obligations which often play a role in investigations related to Domain Name System (DNS) abuse. For example, those related to Registration Data (WHOIS) accuracy in Section 3.7.8 and the Whois Accuracy Program Specification of the RAA (ICANN Compliance often receives reports of inaccurate data associated with allegedly abusive domain names); or those related to zone file third-party access requests (often submitted by security researchers who investigate and help combat DNS abuse) in Specification 4, Section 2 of the RA.

Question 2: Can you describe how the enforcement of these provisions practically takes place from a procedural standpoint, including if there are any unique process elements for DNS abuse related complaints?

ICANN Compliance enforces all obligations with its contracted parties through an established process which provides for a consistent and equal treatment approach.This process comprises two stages: an informal and a formal resolution stage. There are no unique process elements for abuse-related complaints.

The informal resolution stage (through which most investigations are resolved and closed) generally entails, at a minimum, three notifications and two phone calls to the contracted party. These communications include a copy of the complaint(s) received with supporting evidence, an explanation of the specific section(s) of the ICANN agreement/policy involved, and an itemized list of information and records needed to demonstrate compliance. The details of the communications exchanged during the informal stage are confidential. In the event a contracted party continues to be non-compliant after the informal resolution stage is exhausted, ICANN Compliance issues a formal enforcement notice. If the contracted party does not cure all non-compliance areas identified in this formal notice by the specified deadline, ICANN Compliance suspends (registrars only) or initiates termination proceedings (registrars and registry operators) the contracted party's accreditation with ICANN. Formal notices also include an itemized list of actions the contracted party must take to become compliant. Formal enforcement notices are published here.

Question 2 (continued): In addition, besides responding to submitted complaints and performing audits, are there any other mechanisms by which Contractual Compliance identifies actionable information to investigate DNS abuse related complaints?

The actions that ICANN Compliance undertakes to enforce contractual obligations arise from complaints received from external users through the dedicated forms located here, proactive monitoring, and audit-related activities.

ICANN Compliance addresses external complaints related to DNS abuse obligations through the process explained above. Additionally, prior to issuing any notice of breach (concerning any violation even if not abuse-related) to a registrar or registry operator, ICANN Compliance conducts an overall contractual compliance "health check" of the relevant contracted party. During this check, ICANN Compliance proactively reviews the contracted party's website(s) for compliance with the display of mandatory abuse-related information (i.e., RAA 3.18.1 and 3.18.3 for registrars; Specification 6, Section 4.1, for registry operators) and will include the failure to display any of this abuse-related mandatory information in the breach notice with a specific request for the contracted party to remediate the failure by publishing the information required. Similarly, ICANN Compliance will proactively initiate a case with a contracted party where a review of its website or WHOIS response information (for any other reason no related to the issuance of a breach notice) reveals a failure to display mandatory abuse-related information.

In addition, as part of ICANN's review and approval of changes to a Registry-Registrar Agreement (RRA) contemplated in Article 2.9 of the RA, ICANN Compliance reviews RRAs for completeness in terms of content mandated by the RA, including the content mandated by Section 3(a) of Specification 11 of the RA. Where this content is not included or is incomplete, the registry operator is requested to add or complete it.

ICANN Compliance audited its contracted parties on DNS abuse obligations. For example, the registry operator audit focused on DNS security threats that ICANN Compliance conducted from November 2018 through June 2019[1] or the DNS Registrar Abuse Obligations Audit launched on 1 February 2021 and concluded in June 2021[2].

Question 3: Do you have any metrics and/or trends that provide further insight into the complaints that are investigated by Contractual Compliance in relation to DNS abuse?

ICANN has a dedicated public page for Contractual Compliance reporting. This page provides different types of data to the ICANN Community. The first section, referred to as Metrics and Dashboards, provides monthly data.

Beginning in 2018, ICANN Compliance reports included the subject matter category for registrar-related abuse complaints: spam; pharming; phishing; malware; botnets; counterfeiting; pharmaceutical; fraudulent and deceptive practices; trademark or copyright infringement; and registrar abuse contact. The subject matter category was selected by the processor while validating the complaint and represented the abusive activity that the reporter alleged was taking place in connection with the domain name(s).

[1] 17 September 2019 Report published at https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf

[2] 24 August 2021 Report published at https://www.icann.org/en/system/files/files/compliance-registrar-audit-report-2021-24aug21-en.pdf

On 9 March 2022, ICANN Compliance began publishing new reports[3] to help inform ongoing community discussions (including those related to DNS abuse). The new reporting provides more granular data on the complaints received, the obligations enforced, and the process through which these obligations are being enforced. To illustrate historical trends over time, these reports are published as a 12-month rolling series, beginning with the period of January 2021 through December 2021, and an are updated monthly.

These reports can be found at https://features.icann.org/compliance/dashboard/trends-list.

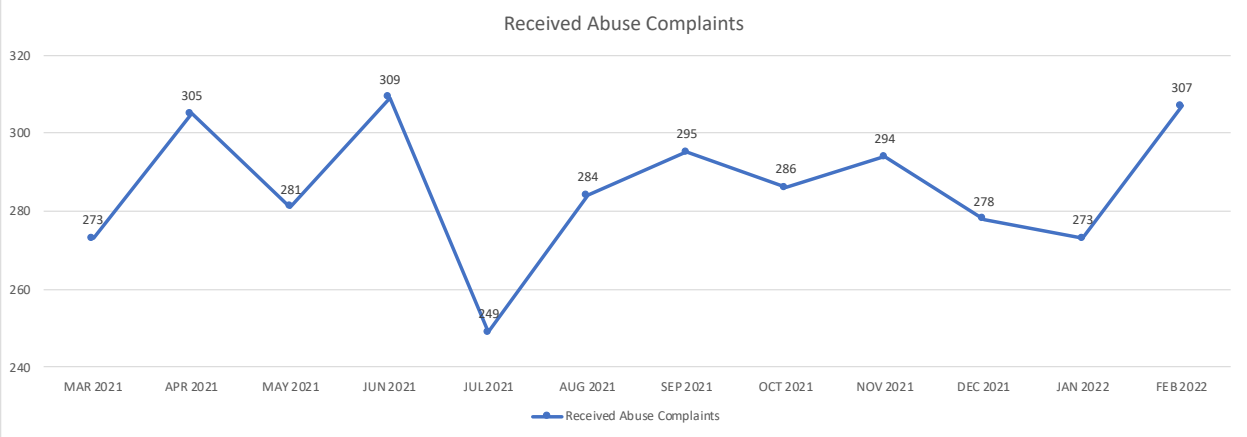
Example of the abuse-related complaints detail report with data from March 2021 through February 2022 below.

The first table shows the volume of abuse complaints received under Section 3.18 of the RAA and details the alleged abuse activity associated with the domain name(s) subject to the complaint (Complaint Categories[4]).

	MAR 2021	APR 2021	MAY 2021	JUN 2021	JUL 2021	AUG 2021	SEP 2021	OCT 2021	NOV 2021	DEC 2021	JAN 2022	FEB 2022	Average
Received Abuse Complaints	273	305	281	309	249	284	295	286	294	278	273	307	286
Complaint Categories													
Pharming, phishing	110	142	109	133	105	110	119	130	127	131	105	153	123
Malware, botnet	37	50	32	39	30	29	31	44	36	40	44	49	38
Spam	64	78	62	67	53	60	79	74	66	68	53	61	65
Counterfeiting	32	35	48	55	29	40	44	54	53	46	35	46	43
Fraudulent, deceptive practices	162	187	163	180	158	179	174	174	180	168	148	170	170
Pharmaceutical	17	9	23	16	21	26	22	14	28	20	16	8	18
Trademark or copyright infringement	102	100	92	117	73	92	103	115	116	103	107	113	103
Abuse contact / procedures information	50	77	44	47	52	46	65	53	49	52	45	57	53
Other	61	63	68	62	58	58	65	59	60	43	55	56	59

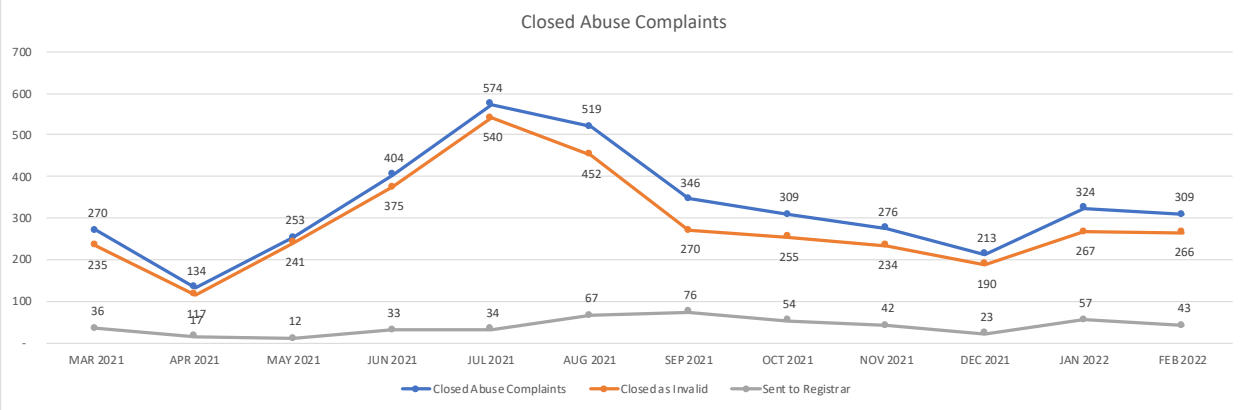
[3] Related blog published at https://www.icann.org/en/blogs/details/new-icann-reporting-enhances-visibility-of-complaint-volumes-and-trends-09-03-2022-en

[4] The complaint categories are selected by the complainant with the submission and are not determined by ICANN Contractual Compliance. One single complaint can include more than one complaint category (e.g., one abuse complaint that involves a domain name that is allegedly used for phishing and to support a botnet infrastructure may result in two complaint categories). Therefore, the sum of all selected complaint categories will not necessarily equal the total number of abuse complaints received within the month. Where the alleged abusive activity does not correspond to any of the specific complaint categories in the chart, the complainant may select the option "Other" (e.g., complaints involving alleged illegal or offensive website content).



The second table shows the volume of closed abuse complaints (also by Complaint Category) detailing those closed without contacting the registrar because of them being out of ICANN's contractual scope versus those closed after obtaining evidence of compliance from the relevant registrar.

	MAR 2021	APR 2021	MAY 2021	JUN 2021	JUL 2021	AUG 2021	SEP 2021	OCT 2021	NOV 2021	DEC 2021	JAN 2022	FEB 2022	Average	%
Closed Abuse Complaints	**270**	**134**	**253**	**404**	**574**	**519**	**346**	**309**	**276**	**213**	**324**	**309**	**328**	100%
Closed as Invalid	235	117	241	375	540	452	270	255	234	190	267	266	287	87%
Sent to Registrar	36	17	12	33	34	67	76	54	42	23	57	43	41	13%
By Complaint Category														
Pharming, phishing														
Closed as Invalid	106	68	91	156	237	174	108	114	109	92	113	129	125	89%
Sent to Registrar	17	8	4	14	11	26	28	20	11	11	21	17	16	11%
Malware, botnet														
Closed as Invalid	42	21	27	49	76	50	33	36	39	24	46	50	41	93%
Sent to Registrar	5	2	0	3	0	3	3	1	2	3	5	4	3	7%
Spam														
Closed as Invalid	68	30	59	86	123	103	77	63	60	52	57	57	70	93%
Sent to Registrar	4	3	1	3	2	6	11	7	1	1	10	6	5	7%
Counterfeiting														
Closed as Invalid	32	23	26	42	100	58	46	46	43	31	40	36	44	90%
Sent to Registrar	5	1	2	5	4	11	8	8	5	2	7	3	5	10%
Fraudulent, deceptive practices														
Closed as Invalid	139	77	140	221	315	286	168	159	149	110	156	138	172	89%
Sent to Registrar	20	6	8	17	14	38	40	25	18	11	33	22	21	11%
Pharmaceutical														
Closed as Invalid	12	9	4	17	33	25	28	7	24	9	16	11	16	80%
Sent to Registrar	5	0	0	1	3	15	6	7	8	1	3	1	4	20%
Trademark or copyright infringement														
Closed as Invalid	69	46	85	104	190	133	101	94	95	62	100	95	98	85%
Sent to Registrar	14	6	9	15	11	25	35	19	19	10	26	19	17	15%
Abuse contact / procedures information														
Closed as Invalid	50	29	48	75	82	81	60	57	46	36	49	54	56	93%
Sent to Registrar	1	3	1	5	6	7	9	4	2	0	2	3	4	7%
Other														
Closed as Invalid	51	23	45	74	122	97	58	53	46	31	47	52	58	89%
Sent to Registrar	1	1	1	4	6	14	12	11	10	3	12	4	7	11%



Question 4: What are the factors that Contractual Compliance takes into account when reviewing a DNS abuse related complaint?

The factors will depend on the details of the complaint and the obligation(s) being enforced.

Specification 6, Section 4.1 of the RA

A complaint regarding a registry operator's failure to comply with the requirements to display abuse-related information on its website will result in ICANN Compliance's review of the website. If the information is missing, deemed incomplete or inaccurate, the registry operator will be required to remediate by publishing the complete, accurate, information and provide evidence that this has been done.

Specification 11, Section 3(a) of the RA

Pursuant to the terms of this provision, ICANN Compliance takes direct enforcement action with respect to registry operators who fail to include the required provision in their agreements with registrars. This includes requesting the relevant registry operator to add the required provision to its Registry-Registrar Agreement (RRA) where it is missing or incomplete (see explanation on page 4 relating to Article 2.9 of the RA).

Specification 11, Section 3(b) of the RA

ICANN Compliance focused a registry operator audit on the review of gTLD registry operators processes and procedures related to the prevention, identification and handling of DNS security threats. Through this audit, ICANN Compliance concluded that most registry operators undertake significant efforts to address DNS security threats - 5% of the registry operators were found non-compliant with Specification 11 3(b) and all of them remediated.

The report providing aggregated results can be found at https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf

Concerning Section 3.18 of the RAA

ICANN Compliance does not review whether the reported domain name is malicious (e.g., whether the domain name is, in fact, being used to conduct the reported activity botnet,

phishing, etc.) Rather, ICANN Compliance validates whether the complainant submitted a fully-formed complaint (includes evidence of a report of illegal or abusive activity submitted to the registrar's abuse-dedicated contact involving a domain name sponsored by the registrar) and if so, whether the registrar complied with its obligations under Section 3.18 of the RAA. Validated complaints are sent to the registrar with an itemized list of the information and records needed to demonstrate compliance.

Question 4 (continued): Are there factors, whether in whole or in part, which are applied across the board ('mandatory') as opposed to on a case-by-case basis ('discretionary')?

As mentioned above, factors applied by ICANN Compliance depend on the details of the complaint and the obligation(s) being enforced.

To address a complaint involving the publication of mandatory abuse-related information, ICANN Compliance will require the contracted party to demonstrate that the information is published, complete and accurate. ICANN Compliance's requests to address a complaint involving whether or how a registrar investigated and responded to an abuse report will include the specific items needed to assess compliance as it pertains to the abuse report. These requests will generally include an explanation - supported by records - demonstrating how the registrar investigated and responded to the abuse reports and, where applicable, whether and to what extent their response was consistent with the registrar's domain name use and abuse policies. Where there is an apparent discrepancy between the actions taken on an abuse report and the registrar's own domain name use and abuse policies, ICANN Compliance will request additional clarification and any evidence needed until such discrepancy is clarified.

Any specific action(s) a registrar decides to take on the domain name(s) and/or their associated accounts in response to abuse reports will depend on the registrar's own domain name use and abuse policies. The RAA does not require registrars to take any specific action on the domain names that are subject to abuse reports. Any action that a registrar may take against a reported domain will depend on the registrar's own policies and review of the details of each case.

Question 4 (continued): Are there any challenges in determining whether a Contracted Party is failing to comply with their contractual obligations regarding DNS abuse? If so, what would assist you in making such a determination?

There are no challenges in determining whether a contracted party fails to comply with the relevant contractual obligations. During an investigation, ICANN Compliance provides the contracted party with a copy of the complaint(s) received with supporting evidence, an explanation of the specific section(s) of the ICANN agreement/policy involved, and an itemized list of information and records needed to demonstrate compliance.

The RAA does not prescribe the specific consequences that registrars must impose on domain names that are subject to abuse reports though. Consequently, ICANN org has no contractual authority to require registrars to impose consequences or take specific actions in these cases.

Similarly, RA Specification 11 3(a) requires registry operators to include a provision in their agreement with registrars, for registrars' agreements with registrants to prohibit registrants from engaging in certain activities (distributing malware, abusively operating botnets, phishing,

piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law) and requiring consequences for the registrants for such activities, including suspension of the domain name. It does not provide the ICANN Organization (Org) with authority to instruct registrars to impose consequences (including suspension) on Registered Name Holders who may be engaging in prohibited activities[5].

In summary, ICANN Compliance does not face any challenges in enforcing the RAA and RA obligations as they are written. If and when new obligations are imposed either through community policy development or new contractual terms, ICANN Compliance will enforce those as well so long as they are unambiguous and enforceable.

Question 5: If you have determined a Contracted Party is failing to comply with their contractual obligations regarding DNS abuse, are there any challenges in effectively remediating the compliance issue? If so, what would assist you to ensure effective remediation?

ICANN Compliance derives its enforcement authority from the agreements between ICANN Org and the contracted parties. Enforcement of these agreements includes the suspension or termination of a registrar's accreditation and the termination of a registry operator's agreement where the contracted party fails to become compliant with the RAA or RA, respectively. There are no challenges in utilizing the tools provided by the contracts. These tools and the length of the processes against noncompliant contracted parties, though, vary depending on whether the noncompliant party is a registrar or a registry operator.

If a registrar fails to become compliant with the abuse-related requirements that are specifically included in the RAA during the informal resolution stage, ICANN Compliance issues a formal notice of breach[6]. If this notice is not cured, ICANN may escalate to a suspension (for up to twelve (12) months) of the registrar's ability to register new domains or accept inbound transfers; or to termination of the registrar's agreement with ICANN.

If a registry operator fails to become compliant with the abuse-related requirements specifically included in the RA during the informal resolution stage, ICANN Compliance issues a formal notice of breach[7]. If this notice is not cured, ICANN may initiate the termination proceedings contemplated by the RA which include mediation and arbitration phases.

[5] Additional details can be found at https://www.icann.org/en/system/files/correspondence/botterman-to-selli-12feb20-en.pdf.

[6] An example of formal notice of breach issued to a registrar for its failure to comply with RAA 3.18 abuse reporting requirements can be found at https://www.icann.org/uploads/compliance_notice/attachment/1173/hedlund-to-yazici-28jan22.pdf.

[7] An example of formal notice of breach issued to a registry operator that included its failure to publish contact details for handling inquiries related to malicious conduct in the TLD (Section 4.1 of Specification 6 of the RA) can be found at https://www.icann.org/uploads/compliance_notice/attachment/1049/serad-to-allain-11jul18.pdf.