12 February 2020

Ms. Claudia Selli
Chair, Business Constituency

Re: Concrete Steps ICANN Org Can Take to Combat DNS Abuse

Dear Claudia,

Thank you for your 9 December 2019 letter regarding DNS abuse discussions at ICANN66. The ICANN Board shares the Business Constituency's (BC's) appreciation for the constructive community dialogue regarding DNS abuse. We agree that DNS abuse is a significant and growing problem and we are heartened by the seriousness with which all segments of the community are attempting to address it.

I would also like to thank you for sharing your analysis and concerns and suggesting concrete steps that the Business Constituency (BC) believes the ICANN organization (ICANN org) can take to combat DNS abuse. The remainder of this letter will focus on the BC's suggestions.

1. Enforce current contract language

The BC suggests that ICANN org can leverage language in the Base Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA) to mitigate DNS abuse.

The BC cites Specification 11 3(a) of the RA which states:

> "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from 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 providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."

The BC also cites RAA 3.18.1 which requires registrars to "take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." The BC reads these two provisions "taken together" to authorize ICANN org to:

> "monitor whether registrars have in fact created a procedure imposing consequences, and do impose these consequences, consistent with applicable law. Should ICANN Compliance determine that these procedures have not been created, or enforced in accordance with their terms, ICANN

Compliance should have the ability to enforce the requirements in RA Section 11.3(a) and RAA Section 3.18.1 as a method of mitigating abuse."

ICANN org, through its Compliance function, enforces the contractual obligations set forth in ICANN's policies and agreements, including RA Specification 11 3(a) and RAA 3.18. The actions that ICANN Compliance undertakes to enforce these contractual obligations are a result of complaints received from external users, proactive monitoring and audit-related activities. Details about some of these actions are described below.

Under RA Specification 11 3(a), registry operators have an obligation to include a provision in their agreement with registrars to prohibit Registered Name Holders (RNHs) from engaging in certain activities, and requiring consequences for the RNHs for such activities, including suspension of the domain. Pursuant to the terms of this provision, ICANN Compliance can, and does, take direct enforcement action against registry operators who fail to include the required provision in their agreements with registrars. However, RA Specification 11 3 (a) does not grant ICANN org an enforcement right against registrars who fail to include the required language in their agreements with RNHs or authority over how, or to determine whether, registrars "do impose these consequences." Instead, RA Specification 11 3(a) provides registry operators and registrars a mechanism to take action against the prohibited activities. In that regard, ICANN org expects registry operators to enforce their Registry-Registrar Agreements (RRAs) with registrars and registrars to in turn enforce their registration agreements with RNHs.

With respect to RAA 3.18, although ICANN Compliance does directly enforce registrars' obligations regarding handling of abuse reports, it does not provide ICANN Compliance the ability to step into the roles of the registry operator or registrar in implementing the mechanism provided by the language in RA Specification 11 3(a).

Instead, RAA 3.18 allows ICANN Compliance to directly enforce the following requirements:

- Take reasonable and prompt steps to investigate and respond appropriately to abuse reports, as required by Section 3.18.1 of the RAA;
- 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 designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office, within 24 hours and by an individual who is empowered to take necessary and appropriate actions in response to the report, as required by Section 3.18.2 of the RAA; and
- publicly display abuse contact information and abuse report handling procedures for users to know how to submit abuse reports to the registrars

(3.18.1 of the RAA) and how those reports would be addressed (3.18.3 of the RAA).

To that end, while investigating abuse report handling complaints, ICANN Compliance often requests the relevant registrar to explain how it investigated and responded to the abuse report and to provide a link to or a copy of the registrar's domain name use and abuse polices that support the registrar's handling of the specific abuse report. 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. However, the RAA does not prescribe the specific consequences that registrars must impose on domain names that are the subject of abuse reports. ICANN org has no contractual authority to instruct registrars to delete or suspend domain names.

2. Prioritize abuse complaint handling

The BC letter observes that ICANN org issued seven breach notices and terminated one registrar over abuse-related issues between January 2014 and September 2019. Based on this observation, the BC appears to conclude that ICANN Compliance does not prioritize DNS abuse-related complaints. However, the BC did not acknowledge ICANN Compliance's enforcement actions taken through its informal resolution process[1] (where the majority of complaints across all complaint types are resolved) or ICANN Compliance audits activities.

To that end, the table below shows the number of registrar abuse report handling complaints received by ICANN Compliance from 1 January 2014 to 30 September 2019 (the time period highlighted by the BC in its letter):

	2014	2015	2016	2017	2018	JAN-SEP 2019	Total
Abuse Complaints	271	438	548	747	787	913	3,704

Below are the number of 1st, 2nd and 3rd notices/inquires sent on registrar abuse report handling complaints to the relevant registrars:

	2014	2015	2016	2017	2018	JAN-SEP 2019	Total
1st Notice/Inquiry	154	160	194	285	271	193	1,257
2nd Notice/Inquiry	82	65	58	55	49	30	339
3rd Notice/Inquiry	24	12	12	3	6	6	63
	260	237	264	343	326	229	1,659

[1] During the informal resolution process, ICANN Compliance works with its contracted parties to help them understand their contractual obligations so they can take steps to demonstrate compliance with those obligations. ICANN Compliance attempts to resolve contractual compliance matters informally before pursuing formal remedies available under the agreements. In the interest of facilitating open dialogue and resolution, the details of the specific contractual compliance activities in the informal resolution phase are not published.

The chart above does not include follow-up communications sent to request additional data or clarifications that occurred between each notice/inquiry phase or the communications that occurred within an ICANN Compliance audit.

The majority of the complaints in the chart above were closed during the informal resolution process because the registrars demonstrated compliance with the RAA's requirements to take steps to investigate and respond to the abuse reports in accordance with the registrar's domain name use and abuse policies.[2] Of those that did not result in breaches, 34% resulted in the suspension of the domain names that were included in the complaint submitted to ICANN Compliance.

Additionally, prior to issuing any notice of breach to a contracted party, regardless of the area of non-compliance that led to the issuance of the breach notice, ICANN Compliance conducts an overall contractual compliance "health check" of the contracted party. During this check, ICANN Compliance reviews the relevant registrar's website(s) to confirm, among other things, that the abuse contact information and abuse report handling procedures description are published, as required by RAA 3.18. Issues found during these checks are included in the breach notice and required to be cured for the contracted party to maintain its accreditation with ICANN.

As a result of health checks conducted from 1 January 2014 to 30 September 2019 (the time period highlighted by the BC in its letter), ICANN Compliance issued 42 breach notices to registrars which included notices for failures to publish on the relevant registrar's website an email address to receive abuse reports and/or a description of the registrar's procedures for the receipt, handling and tracking of abuse reports, as required by Section 3.18.1 of the RAA and Section 3.18.3 of the RAA, respectively. In resolving these breach notices, ICANN Compliance further issued:

- Five (5) notices of termination of the registrar's accreditation; one (1) registrar voluntarily terminated its accreditation upon receiving the notice of breach.
- Four (4) notices of suspension of the registrar's accreditation.

ICANN Compliance has also focused its recent audits on abuse. The registry operator audit conducted from November 2018 through June 2019[3] focused on

[2] Examples of steps taken by registrars in response to abuse reports: contacting the registrant of the domain name(s) subject to the abuse report and asking for and obtaining evidence disputing the alleged abuse (e.g. licenses for pharmaceutical-related abuse reports); providing web-hosting information about the subject domain name(s) to the complainant for reporting the abusive content to the entity hosting the allegedly abusive content; terminating the agreement between the registrar and registrant by allowing the transfer to a different registrar; and/or suspending the domain name.

[3] 17 September 2019 Report published at https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf

Domain Name System (DNS) security threats, including domain names used for phishing, malware and botnets. ICANN Compliance is currently preparing to launch the registrar audit which will also focus on DNS security threats.

The above illustrates that ICANN Compliance does prioritize addressing abuse report handling complaints by not only addressing external complaints, but also by conducting proactive monitoring on compliance with the existing contractual requirements through audit activities.

The BC further states that, "ICANN Compliance needs to shift from a model driven on churning through a high number of low impact issues (and tickets) to focusing on issues that present real threats to the security of the DNS and cause actual harm to consumers, businesses, governments, and NGOs." This comment suggests that the BC did not take into consideration the overall activity of ICANN Compliance in addressing more than 25,000 complaints annually; enforcing ICANN policies and agreements intended to protect registrants rights such as those prescribing inter-registrar and inter-registrant transfers or domain renewal requirements; those related to WHOIS accuracy data (often used to report inaccurate data associated with allegedly abusive domain names); or those related to zone file third-party access requests (often used by security researchers who investigate and help combat DNS abuse).

From December 2018 to December 2019, ICANN Compliance received 26,233 complaints, with the following complaint types making up more than 80 percent[4] of the total complaint volume for the 13-month period:

Abuse:	1,506 (5.7% of total complaints)
Domain deletion:	740 (2.8%)
Renewal:	1,035 (3.9%)
Transfer:	4,162 (16%)
Whois Inaccuracy:	12,588 (48%)
Zone File Access:	1,550 (5.9%)
Total:	21,581 (82%)

Abuse, Whois Inaccuracy and Zone File Access complaints account for almost 60 percent of the total complaints submitted. Domain Deletion, Renewal and Transfer complaints account for approximately 20 percent of the total.

It is not clear which of these complaint types ICANN Compliance should "de-prioritize," or on what legal or policy basis any of these complaints could be de-prioritized. ICANN org would be interested in any specific suggestions that the BC might have in this regard.

[4] The remaining 34 complaint types account for less than one ticket per day, each.

Finally, the BC recommends that ICANN Compliance focuses its efforts on "contracted parties that operate in bad faith by either specifically marketing their services to bad actors or by engaging in bad acts that are prohibited under the RA and RAA themselves." ICANN Compliance derives its enforcement authority from the agreements between ICANN org and the contracted parties (registry operators and registrars). Enforcement of these agreements already includes the ability of ICANN org to suspend (for registrars only), terminate or not renew a contracted party's agreement[5] where the contracted party fails to demonstrate compliance with the RA or RAA. However, these agreements do not define the operative terms or conditions described in the BC's suggestion, including, what exactly it means in all situations to "operate in bad faith;" or "specifically marketing…services;" and who are the "bad actors." As a result, there does not appear to be any contractual authority for ICANN Compliance to take the actions recommended by the BC beyond enforcing RA and RAA provisions, which ICANN Compliance currently does. If the BC believes such authority lies elsewhere in ICANN policies and agreements, ICANN org would be interested in the BC's analysis.

3. Strengthen Contracts

The BC next asserts that ICANN org is a third-party beneficiary of the Registry-Registrar Agreement (RRA) and cites one RRA to support its assertion.[6] However, ICANN org does not have third-party beneficiary rights to enforce terms in the RRA. It is not clear why this particular RRA contains language indicating that ICANN is a third-party beneficiary - neither ICANN org nor the Registry Agreement requires registry operators to include this language in their RRAs or claim that ICANN is a third-party beneficiary.

The BC's statement "if ICANN Org believes it is unable to meaningfully enforce current language, as has been suggested […]" is also not accurate. ICANN org has neither stated nor suggested that it is unable to meaningfully enforce its agreements with contracted parties. ICANN Compliance enforces the contractual obligations set forth in ICANN's policies and agreements, as explained throughout this letter. Beyond those terms explicitly required by the Registry Agreement to be included in the RRA (e.g., Specification 11 3(a)), the RRA is a voluntary agreement between registry operators and registrars and its terms are not binding on ICANN org (who is not a party to the RRA).

If the BC believes additional contractual requirements are necessary, ICANN org encourages the BC to continue actively participating in the policy development processes. Any requirements incorporated into an ICANN policy or agreement will be enforced by ICANN Compliance.

[5] Formal enforcement notices are published at https://www.icann.org/compliance/notices.
[6] On page 3 of the BC's 9 December 2019 letter they provide the example of: "See, e.g., Article 10.4 of .OVH RRA: "Article 10.4. Third-Party Beneficiaries The Parties expressly agree that ICANN is an intended third-party beneficiary of this Agreement."

4. Clarify action steps for registrars

The BC suggests that the Board direct ICANN org to issue an advisory clarifying the requirement in RAA Section 3.18 for registrars to take "reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." ICANN Compliance attempted to provide some clarification on this topic in a previous blog. The blog noted that there were "considerable differences of opinion among members of the multistakeholder community regarding what constitutes an appropriate response to an abuse report." Nevertheless, for parties that submit a valid abuse report,[7] they could reasonably expect registrars to undertake, "at least the following steps in response to a report of abuse or illegal activity, absent extenuating circumstances or reasonable justification:

1. Acknowledge receipt of the complaint.
2. Look at the specific url(s) that are alleged to be the source of the abuse or illegal activity. (Examples of extenuating circumstances or reasonable justification for not doing so might include, for example, where the url is alleged to contain child pornography and accessing the content might subject the registrar to liability, or where the registrar might expose itself to malware by accessing the url.)
3. Promptly notify the registered name holder of the complaint, or where the name was registered through a reseller, notify the reseller and ask the reseller to notify the registered name holder of the complaint.
4. If submitted by the complaining party, consider and evaluate any formal determination by a court, regulatory authority or law enforcement agency regarding abuse or illegal activity. In doing so, the registrar may choose to take into account considerations such as jurisdiction and due process.
5. Communicate to the complaining party the substance of any response to the abuse report that is provided to the registrar or reseller by the registered name holder.
6. Communicate to the complaining party, within a reasonable period of time, the registrar's position and what actions, if any, the registrar proposes to take."

It should be noted that the above serves as guidance and is not contractually binding. The RAA does not define, with any specificity, what "reasonable and prompt steps to investigate and respond appropriately" means. Nor does the BC letter specify what kinds of clarifications are necessary, or what problems an advisory on "investigate and respond" might solve. We would therefore encourage the BC to enter into discussions with the Registrar Stakeholder Group and/or individual registrars to define the problem set and develop best practices. ICANN org would be happy to facilitate these discussions if requested by the parties.

[7] The blog also listed criteria that valid reports of abuse or illegal activity should meet in order for registrars to fulfill their obligation to investigate and respond.

5. Improve the Compliance complaint submission process

The BC suggests a number of changes to the process for submitting complaints to ICANN Compliance.[8] These suggestions are helpful as ICANN Compliance prepares to migrate to a new complaint processing system that will enable the use of "smart forms" for the submission of complaints. The smart forms will help complainants easily identify the relevant complaint type as well as the information or evidence needed to accompany the complaint. The smart forms will also provide more information to complainants, to illicit more relevant information, and allow for more efficient processing of the complaints and more granular public reporting of how complaints were addressed.

Finally, the BC recommends that ICANN org should implement an escalation or appeals process that can be invoked by complainants who disagree with the outcomes of their complaints. While the primary focus of ICANN Compliance's function is to enforce ICANN's policies and agreements (even if the result is not the desired outcome by the complainant), complainants can reply back to an in-process compliance ticket to express concerns or disagreement, or to request clarifications. Additionally, a closure note – that includes an email address to use for post-closure questions and a customer satisfaction survey link – is sent to each complainant (and contracted party) when a compliance ticket is closed. Each survey's comments and the corresponding compliance ticket(s) receive reviews by multiple team members within ICANN Compliance. This review may result in additional clarification being sent to complainants (or contracted party), where needed; or the re-opening of closed tickets, where warranted. Complainants can also escalate their concerns to the ICANN Senior Vice President of Compliance and Consumer Safeguards, or seek review with the Complaints Officer, the Ombudsman, and/or the ICANN Board through the Reconsideration process. Given the existing escalation processes and the fact that they are not intended to be a substitute for the policy development process or address concerns about ICANN Compliance's contractual remit, it would be helpful to understand the basis for the BC's concern and the rationale for creating a new accountability mechanism.

Thank you again for sharing your concerns and suggestions. I hope you find this response to be useful and look forward to your further thoughts.

Sincerely,

Maarten Botterman
Chair, ICANN Board

[8] See Annex A of the BC letter.