9 December 2019

Maarten Botterman, Chair
Members of the Board of Directors
Internet Corporation for Assigned Names and Numbers (ICANN)

Dear Chairman Botterman and Members of the Board:

The Business Constituency (BC) greatly appreciates the community-wide and board discussions regarding DNS abuse during ICANN66 in Montreal. We thank you and our ICANN colleagues for this constructive engagement. The purpose of this letter is to recap key takeaways from these discussions and to highlight expeditious ways in which ICANN Org, with Board oversight, can take concrete steps to more effectively combat DNS abuse through existing mechanisms in both the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts.

Key Takeaways from ICANN66

1. DNS Abuse is a significant[1] and concerning issue for the entire ICANN community.
2. There is community-wide consensus that the above-listed abuses pose significant threats to consumers and the security of the DNS, and the mitigation of these forms of abuses should be prioritized by ICANN Org.
3. ICANN has the opportunity to utilize its contracts for enforcement purposes, and to strengthen agreements with registries and registrars in a way that removes ambiguity and provides ICANN Org with more effective enforcement mechanisms.
4. We must bolster ICANN's resources in the Compliance department to ensure accountability by the contracted parties in addressing harmful DNS abuse.

DNS abuse as a concern

DNS abuse is a significant concern not only to our constituency, but also to the Governmental Advisory Committee and others. We applaud proactive steps to combat abuse (particularly DNS security threats), such as the recent framework to address abuse as proposed by a number of contracted parties, but believe more must be done if abuse is going to be meaningfully addressed. The ICANN Board has a fiduciary duty to ensure that ICANN Org lives up to its commitments under the Bylaws to "preserve and enhance the…operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet." The BC believes the ICANN Board must take a more active role in ICANN's

1 As documented in the BC's Statement on DNS Abuse:

- The global cost of cybercrime is rising, and reached an estimated $600 billion in 2018, according to the Center for Strategic and International Studies, in partnership with McAfee.
- The Anti-Phishing Working Group (APWG) reported a total number of detected phishing sites in the second quarter of 2019 of 182,465, up sharply from the 138,328 reported in the fourth quarter of 2018.
- Akamai reports a strong uptick in phishing attacks against consumers.
- Global insurance giant AIG reports that phishing attacks have now outpaced ransomware as the most frequent instances of fraud, alarming the business community and security experts.

mitigation effort, and accordingly must take advantage of all possible avenues for making the DNS and the Internet stable and secure.

Concrete Steps ICANN Org Can Take to Combat DNS Abuse

Enforce current contract language

In the immediate term, ICANN should proactively use existing tools within the RA and RAA to mitigate DNS abuse. The RA and RAA, particularly when taken together, outline:

- An obligation for registries to require registrars to include language in registration agreements prohibiting certain types of security threats;
- An obligation for registries to require registrars to include consequences for registrants who engage in prohibited abusive activities, up to and including suspension of the domain name; and
- Requirements for registrars to take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

More precisely, Specification 11.3(a) of the RA (with emphasis added):

> ***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.***

Further, the RAA includes useful abuse mitigation language in Section 3.18 (emphasis added):

> *3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.*
>
> *3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time).* ***Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.***

This language provides an avenue for mitigation of very specific types of abuse.

However, we learned at ICANN66 that ICANN Compliance narrowly construes this language as only requiring specific terms to be included in the registration agreement itself, but not requiring enforceable action on the registrar's part via the registration agreement.

However, this interpretation appears to ignore the second part of the section that requires "consequences for such activities, including suspension of the domain name." We note that imposition of consequences would need to be "consistent with applicable law and any related procedures," so some violations may require immediate suspension, while it may be sufficient to defer to existing legal

mechanisms for other violations.

We suggest that ICANN Org 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.

Prioritize abuse complaint handling

Curiously, despite agreement in the ICANN community that DNS abuse is a significant and growing problem, and ICANN having contractual tools to hold contracted parties accountable for prohibiting registrants from engaging in certain abusive activities, ICANN's compliance department issued only seven breach notices and terminated one registrar over abuse-related issues between January 2014 and September 2019.

Without context, one may conclude that all registries and nearly all registrars are complying with the terms of their contractual agreements with ICANN, and that consequently, DNS abuse is a trivial issue. However, ICANN's own audit reports note that the second most common registrar deficiency is non-compliance with even the most basic elements of Section 3.18 of the RAA – such as publishing an abuse contact and actually monitoring that mailbox.

ICANN Org, simply put, must prioritize the handling of DNS abuse-related complaints. 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. ICANN Compliance must now focus its efforts more precisely, including 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.

Strengthen contracts

ICANN Org is a third-party beneficiary of the Registry-Registrar Agreement (RRA)[2], and can take action based on that status.

Despite the above, if ICANN Org believes it is unable to meaningfully enforce current contractual language, as has been suggested, it is further incumbent upon the ICANN Board to direct ICANN Org to proactively seek the necessary amendments to the RAA. ICANN's current negotiations with registrars to amend the RAA to address the adoption of RDAP presents ICANN Org with the perfect opportunity to clarify this language.

2 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."

Clarify action steps for registrars

The BC calls on the Board to direct ICANN Org to issue an advisory that clarifies what is meant by "reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." ICANN may initially wish to look to the framework to address abuse for guidance on what constitutes "reasonable and prompt steps" with regard to particular forms of DNS abuse. The BC also notes that such an advisory has already been issued with respect to Specification 11 (3)(b).

Improve the Compliance complaint submission process

Regrettably, ICANN's website is an unhelpful resource with regard to submitting a DNS abuse-related matter. Navigation sends the user haphazardly over the site, including links to Contractual Compliance and ICANN's complaints office before an assumedly skilled user could arrive at the correct page and link. Even a link from the complaints office web page leads to a submission form more appropriate for ICANN Compliance.

In order for all users to have prompt access to this resource and, importantly, to more accurately measure the true scale of the DNS abuse problem, the BC suggests the changes outlined in Annex A of this letter.

Take action on overdue matters

A topic related to DNS abuse is the enabling of better tools in ICANN's arsenal that were developed by the community but have not yet been put to use, or even acted upon. Reticence on ICANN's part is causing real harm to internet users as abuse rates continue to rise. ICANN Org's refusal to implement Board-approved policies and contractual requirements raises very serious corporate governance concerns that should not be ignored by the ICANN Board.

For instance, ICANN's GNSO Council unanimously supported an accreditation policy for privacy/proxy service providers, and the ICANN Board approved the policy in August 2016 -- *more than three years ago*. Since then, implementation of a policy that affects tens of millions of registrations has stalled. It simply is unacceptable to stop work altogether -- the ICANN Board must demand that ICANN Org restart this implementation immediately and develop a clear plan describing the pending issues and a short timeline for resolving them.

The same is true of ICANN's now aged effort to bring cross-field validation to the registration data system, which is needed to improve the accuracy of WHOIS data. ICANN Org issued a Request for Information on Contact Data Validation and Verification Systems in February 2014, *nearly six years ago*. Recognizing that data accuracy is an important component of GDPR compliance, the ICANN Board again must direct ICANN Org to finally execute on what will become a critical tool in the fight against DNS abuse.

Next Steps

It's clear that at every level, all parties in the domain name registration chain are concerned with and have a role in mitigating abuse. The BC believes that ICANN Org is overdue for recognizing and exercising its own role. Our proposed improvements are common sense suggestions that will directly

target types of DNS abuse already identified via community-driven processes. We hope the ICANN Board will instruct ICANN Org to implement these improvements.

We look forward to your reply.

Sincerely,

Claudia Selli, Chair
The ICANN Business Constituency

Annex A: Suggested changes to submission process

1. Make links to Compliance complaints more prominent at the ICANN.org home page.
2. Align wording on Complaints Office page and complaint submission form.
3. Update Compliance page to include a section specifically for defined forms of DNS abuse.
4. Create a DNS abuse reporting mechanism that specifically asks the complainant about the following:
    a. What is the domain name involved?
    b. Is this issue related to? (allow multiple selections)
        i. pharming
        ii. phishing
        iii. distributing malware
        iv. operating botnets
        v. piracy,
        vi. trademark or copyright infringement,
        vii. fraudulent or deceptive practices,
        viii. counterfeiting,
        ix. otherwise engaging in activity contrary to applicable law
    c. Have you contacted the registrar directly and allowed a reasonable amount of time to respond?
        i. If no: the form should provide a single click mechanism to get to the right page on the registrar's site or provide the correct, registrar-specific abuse contact email address.
    d. Did you receive a response to your abuse complaint?
    e. What was the registrar response, including any steps taken to mitigate the abuse?
5. Publish response rates for complainants.
6. Implement an escalation or appeals process that can be invoked by complainants who disagree with the outcomes of their complaints.