655 Third Avenue, 10th Floor, New York, NY 10017-5646, USA
t: +1-212-642-1776 | f: +1-212-768-7796
inta.org

INTA Comments on the Base gTLD RA and RAA Amendments

1. Introduction

The International Trademark Association (INTA) is pleased to have the opportunity to provide ICANN with input on the Amendments to the Base gTLD Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) to Modify DNS Abuse Contract Obligations (the Amendments). INTA applauds the Contracted Parties for initiating negotiations with ICANN to create more accountability and definitive steps for fighting the ongoing problems in the area of domain name abuse. INTA supports the passage of the Amendments. We recognize this is a good first step to improve compliance and accountability for combating a complex set of technical and legal issues surrounding domain name system abuse ("DNS Abuse").

2. Areas for Improvement and Continued Consideration

While INTA supports the Amendments, we do feel that there is room for more clarity and improvements either now or as we continue to think about realistic, measured approaches to meet the needs of contracted parties and end users. Our comments on webforms improvements should be incorporated now to allow registrars to gather comprehensive evidence and avoid prejudice to reporters. Our comments on more complex areas like abuse definitions may have to wait until future negotiations. They should be seriously considered given the evolution of technology and the new ways in which domain names are being abused.

a) Addition of Webforms for Reporting DNS Abuse

Both the RA and RAA are amended to add that webforms, in addition to an email address, may be used to report DNS Abuse. However, webforms can, and have been used, to prejudice those who report abuse. For example, webforms may have very low character limitations for reporters and may not allow the uploading of attachments containing evidence of abuse. We recognize that webforms are helpful for Registrars to streamline reporting and we support their use, but the webforms must allow reporters to present full reporting of alleged abuse and the submission of evidence. The Amendments should include reasonable standards for word/character limits and the ability to provide attachments in a variety of common formats like .jpeg and .pdf. It would be helpful to consult reporters as to what reasonable limits are and the capability of the Registrars to accommodate those limits.

b) Narrow Definition of "DNS Abuse"

Both the RA and RAA are being amended to include the definition of "DNS Abuse" that has been adopted by the Voluntary Framework and the Domain Name Abuse Institute. This definition reads as follows:

> *[M]alware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section as those terms are defined in Section 2.1 of SAC115.*

While INTA agrees that a definition is necessary to ensure proper compliance. The proposed definition does not include deceptive, malicious, or other illegal acts such as cybersquatting, typosquatting, trademark infringement, sale of counterfeits, domain spoofing, and content piracy. Consequently, this proposed definition excludes significant portions of consumer protection and intellectual property law. End users could be unintentionally denied their rights to redress given the limitations of the scope of the definition.

Moreover, the Amendment cites SAC115 as the source of its definition. However, SAC115 specifically states under 1.2.1:

> *To be clear there are additional abuses that are worthy of discussion.* ***SSAC finds some of the specific definitions limited, and the above do not provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time***. (Emphasis added by INTA.)

The definition, as proposed in the Amendments, is unnecessarily limited to a small number of technical violations. It allows bad actors to perpetuate fraud and steal from consumers through trademark infringement and piracy. While INTA notes that the proposed definition will address a small number of harms more concretely, the definition does not recognize the true state of play in the DNS.

DNS Abuse is a significant threat to global enterprises and consumers. Domain names are often considered the digital front door that customers and business partners associate with a company's products, email communications, and corporate persona. Thus, the inclusion of acts including intellectual property infringement and misuse within the definition of DNS Abuse is vital to mitigating and preventing all forms of DNS Abuse.

In order to protect online users, consumers, and intellectual property, DNS Abuse should be defined in a way that encompasses a broader range of harms. Thus, in response to this need, the INTA Board of Directors has adopted the following definition of DNS Abuse:

> *Any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity.*

The full Board resolution and rationale may be accessed here. The benefit of adopting this definition is that it encompasses the proposed definition in the Amendments. This a

good solution for solving the problems of abuse because it focuses on intention. Intentional bad acts associated with domain name use require robust tools for measured actions. This is the best way to protect end users whether domain owners, intellectual property owners, or consumers.

In the event that the negotiating parties are not ready to adopt the full INTA definition, it is important that, at a minimum, the term "illegal activity" be added in the Amendments to broaden the bad acts that the RA and RAA capture. "Illegal activity" is defined within the RAA as:

> *Conduct involving use of a Registered name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.*

Illegal activity must be included as a form of domain abuse as it is a key responsibility of the contracted parties not only to ensure the stability and interoperability of the Internet but the security as well. Security encompasses safety. We all have a duty to protect end users from harm.

c) Confronting Abuse at Scale

The proposed Amendments do not consider that DNS Abuse is frequently perpetrated by one party through multiple domain names. The Amendments should therefore consider how DNS Abuse may be efficiently mitigated by addressing abuse by a "party" rather than by each domain name. This may be done by requiring Registrars to suspend or terminate accounts after a "party" or "account" has received or been the subject of a set number of reported and verified cases of DNS Abuse. Moreover, there should be an obligation for Registrars to share data regarding known perpetrators of DNS Abuse to prevent those perpetrators from engaging in DNS Abuse across different Registrars.

d) Definition of Actionable Evidence

The RAA is amended to include:

> *When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*

Similarly, the RA is amended to include:

> *Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a*

minimum, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action, by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

The Amendments do not define "actionable evidence." This language is therefore indefinite and produces uncertainty that may lead to failures to address abuse because of an unclear bar. The standards of what is "actionable" should be clear within a range of enumerated types of "actionable" evidence including format, volume or other factors that are determined based on consultations with reporters. Reporters and contracted parties should have common understandings so that one side is not overwhelmed with unhelpful evidence and the other side is not frustrated if action is not taken.

Moreover, the uncertainty of what is considered "actionable evidence" ties into concerns regarding the use of Webforms for reporting DNS Abuse because a Registrar or Registry may use a Webform with limitations that make it difficult to provide what is unclearly defined as "actionable evidence." "Actionable evidence" should be defined in a way that includes evidence that is easily and reasonably accessible to reporters.

e) Definition of "Appropriate Mitigation Actions"

Additionally, while the Amendment to the RA includes the minimum "mitigation action(s)" that a Registry must make when a registered domain name is used for DNS Abuse, the Amendment to the RAA does not specify what is considered "appropriate mitigation action(s)" that a Registrar must take. This term should be defined within the Amendment to the RAA to prevent abuse and encourage action from the Registrar. The language should also reference and obligate parties to abide by future consensus policies that are developed.

f) Referring Actions: Registries and Registrars Obligations/Timeframes

The Amendment to the RA requires the Registry to refer reports of DNS Abuse to the sponsoring Registrar. However, there is no obligation for the Registry to act to mitigate DNS Abuse in the event that the Registrar does not. This should be an obligation of the Registry.

The RA and RAA should also be amended to require the Registrar or Registry to inform the reporter of what actions have been taken after a DNS Abuse report has been filed and found to include "actionable evidence." These changes aim to encourage action from Registries and Registrars when DNS abuse is reported.

The Amendments to the RA and RAA do specify that Registrars and Registries must take prompt mitigation action. However, there should be a specific timeframe in which they must respond to DNS Abuse reports due to the urgent nature of these threats. Registrars and Registries should be obligated to respond within 48 hours of receipt of a credible DNS Abuse report.

g) Remedies/Escalation

Both the RA and RAA have been amended to include sections on DNS Abuse mitigation efforts by Registrars and Registries. However, both Amendments lack language defining what actions may be taken if a Registrar or Registry fails to take appropriate mitigation actions. The Amendments should include specific remedies if a Registrar or Registry fails to act. Such Amendments should be incorporated into the contracts themselves to aid in enforceability.

Moreover, the Amendments should include language on how a reporter may escalate an issue if a Registrar or Registry fails to act. Clear guidelines would allow ICANN to have instructions on how to enforce failure to comply when fielding complaints from reporters regarding Registry or Registrar inaction. The Amendments should also include language that grants the ICANN Contractual Compliance authority with the responsibility and power to enforce against Registrars and Registries that continue to harbor DNS Abuse and fail to act.

3. Conclusion

INTA appreciates the opportunity to share our comments and suggestions regarding the Amendments. As mentioned above, we applaud this important step in clarifying the contractual obligations for Registrars and Registries. As far as we have gotten in this effort, we also recognize that there is more work to go. With regard to our suggestions for clarifying definitions and obligations more precisely, we recommend that as many as possible be incorporated into the main documents now. Some of our concerns may also be appropriately addressed in the Draft Advisory guidelines. We recommend that the Draft Advisory become an evergreen document as best practices and common understandings are developed between reporters, contracted parties and ICANN.