CPH TRUSTED NOTIFIER FRAMEWORK

OVERVIEW

For several years now, Trusted Notifiers have been relied upon by many registries and registrars to address both DNS Abuse[1] issues as well as website content abuse questions that fall within their respective policies. The Framework to Address Abuse stated, "[b]efitting their designation, Trusted Notifiers earn the registries' and registrars' trust with a recognized subject matter expertise, an established reputation for accuracy, and a documented relationship with and defined process for notifying the registries and registrars of alleged abuse. While it is ultimately the responsibility of the registries and registrars to take action on verified forms of abuse, Trusted Notifiers can serve as a crucial resource to enhance the abuse monitoring and disruption procedures of registries and registrars."[2]

PURPOSE OF THIS DOCUMENT

This voluntary framework is intended to serve as a guide for parties considering entering into Trusted Notifier arrangements. This framework is also intended to explain the role, responsibilities, and expectations of Trusted Notifiers, in the mitigation of abuse—both DNS Abuse and website content abuse. The document is drafted by the Registries and Registrars Stakeholder Groups.

TRUSTED NOTIFIER

I. **Role and Expectations**

A Trusted Notifier is an entity that enters into a written agreement with a registry or registrar (each, a "Registration Provider") that outlines the roles and responsibilities of the Trusted Notifier and the Registration Provider around handling reports of abuse.

In general, a Trusted Notifier is an entity that:

[1] "DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse)", Various Authors, "The Framework to Address Abuse," at 4-5, October 2019, https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf

[2] Ibid

- has a strong, demonstrated expertise in the subject matter;
- operates with a consistent adherence to a high level of substantive and procedural due diligence;
- stands behind its reporting and is committed, in writing[3], to a low false positive rate and the accuracy of its notices; and
- has a clearly enumerated process for registrants to challenge the Trusted Notifier's recommendations.

Not all Notifiers are Trusted Notifiers

Internet and Jurisdiction (I&J) notes that, when it comes to vetting potential Trusted Notifiers, "no external 'accreditation' mechanism exists to certify their credibility and they currently only have the authority that [Registration Providers] accept to bestow upon them."[4] This reflects a core principle: no individual or organization is, simply by their expertise, a Trusted Notifier[5]; that status is only conferred when a Registration Provider agrees to put such trust into the notices from that notifier—and that status is only conferred with respect to Registration Providers with such agreements with that notifier. I&J notes that this trust is based on credibility and accountability, noting "the overarching criterion […] is reputation over time: how long the notifier has been active, its track record on the market and, more importantly, whether it is willing to defend its notices and stand by the operator in case of litigation." [6]

Choice of Action is the Prerogative of the Registration Provider

A Trusted Notifier's notice need not be a substitute for a Registration Provider's judgment; instead, the Registration Provider may accord the notice from the Trusted Notifier with a heightened level of deference but still take steps necessary to ensure

[3] Memorandum of Understanding (MOU) or legal contract.
[4] *Internet and Jurisdiction Policy Network, Domains and Jurisdiction Contact Group*, "Operational Approaches, Norms, Criteria, Mechanisms," at 8, April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf
[5] In general, any entity or individual that reports a potential abuse case is a notifier or reporter. These entities include courts from local jurisdictions, courts from foreign jurisdictions, specialized notifiers (e.g., LEA, government agencies, cybersecurity organizations, etc.), concerned individuals, and members of the public. However, these reporters are not considered Trusted Notifiers simply by way of their expertise.
[6] *Internet and Jurisdiction Policy Network, Domains and Jurisdiction Contact Group*, "Operational Approaches, Norms, Criteria, Mechanisms," at 8, April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

that the processes set forth in its written arrangement were followed and that the notice seems credible and accurate.

Trusted Notifier's Relationship with Registration Providers

Typically, Trusted Notifier arrangements are codified in writing between each individual Registration Provider and the notifier. This arrangement should provide a level of understanding and comfort to the Registration Provider as to the Trusted Notifier's processes and due diligence, and vice-versa. Since there are potential legal ramifications and exposure to taking action at the DNS level (particularly to remedy issues that are outside ICANN's remit), these arrangements should also address apportionment of liability. Registration Providers or a Trusted Notifier may see fit to include representations and warranties and/or indemnification provisions, to incentivise expectations of transparency, due diligence and ensuring that actions taken based on the notice of a Trusted Notifier, particularly in situations where the notice was to protect commercial interests, were appropriately and properly made.

A Registration Provider may enter into a Trusted Notifier arrangement with a third-party expert organization for any abuse of its namespace covered by its applicable policies (e.g., Acceptable Use Policy, Terms of Service, or Anti-Abuse Policy). The Internet and Jurisdiction Policy Network's *Operational Approaches, Norms, Criteria, Mechanisms*[7], sets forth several factors a Registration Provider should consider in contemplating such a potential relationship, foremost among them being trust.

II. Due Diligence by Trusted Notifiers

Acting at the DNS level has a major impact on the domain name, the services that rely on it, and the registrant. Therefore, any action that may disrupt the resolution of a domain name requires the utmost care and attention to *substantive* and *procedural* due diligence. In some cases, the collateral damage from acting on a false positive may be worse than the suspected abuse. Trusted Notifiers, as subject matter experts, are expected to conduct thorough due diligence before sending an abuse notice to Registration Providers. Not doing so could result in a higher rate of false positive

[7] *Internet and Jurisdiction Policy Network, Domains and Jurisdiction Contact Group*, "Operational Approaches, Norms, Criteria, Mechanisms," at 8, April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

reports—and damages to the internet ecosystem—which may lead to the notifier losing its "trusted" designation.

Substantive Due Diligence

Substantive due diligence means making certain that the alleged abuse is properly investigated, substantiated, and documented[8]. To the extent it is legally possible[9], this documentation must be immediately made available to the Registration Provider and any impacted party (that is, the documentation should be provided, upon request, to a registrar if the registry takes action or to the registrant if a registrar takes action).

Procedural Due Diligence

Procedural due diligence ensures that an alleged abuse is reported to the party who is best positioned to act. For DNS Abuse, abuse notices may be sent to Registration Providers. For website content abuse, abuse notices should be made in the following order: website operator → registrant → hosting provider → registrar → registry.

Notwithstanding the foregoing, a Registration Provider and a Trusted Notifier may mutually define their own thresholds for substantive and procedural due diligence.

III. Transparency

Trusted Notifiers and Registration Providers may consider it appropriate to provide a level of transparency into their relationships to improve visibility into the registration provider's policies and identify paths for recourse for impacted parties. For instance, the I&J notes "a two-dimensional approach" to address concerns about transparency around notifiers by 1) sharing statistics on abuse reports and actions taken, and 2) publishing the decision-making criteria (e.g., abuse policy, thresholds for action), abuse point of contact and procedure to appeal or request recourse. However, whether a Registration Provider and Trusted Notifier are in a position to provide this insight, and the detail that can be provided will depend on a variety of factors. These factors include, but are not limited to, the subject matter, risk of creating attack vectors, and the public

[8] https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-113-Due-Diligence-Guide-for-Notifiers.pdf

[9] In some limited circumstances (e.g., child sexual abuse material) it may be illegal for another party to review the Trusted Notifier's due diligence documentation; notifiers of these types of content should have mechanisms for ensuring substantive due diligence of their assessments (e.g., formal quality assurance processes, external judicial review mechanisms).

interest in the arrangement. Any transparency or reporting measures should be agreed upon by the parties.

IV. Potential Future Work

As the number of contracted Trusted Notifiers grows, it is possible that Registration Providers will be challenged in their respective ability to scale administrative and operational engagement to desired levels. As such, the Contracted Party House will consider potential optional mechanisms and relationships that could deliver economies of scale, while allowing each Registration Provider to continue to exert their own judgement over their respective Trusted Notifier agreements, policies, and any course of action taken.