ICANN | RrSG
Registrar Stakeholder Group

Guide to Registrar Abuse Reporting Practices

Introduction and purpose

This document presents guidelines for submitting an abuse report to a domain name registrar. **There are a range of activities collectively identified as abuse, including, phishing, spam, malware, and trademark and copyright infringement.**

Most countries have laws that regulate hosting and website publishing activities, and these laws often include mandatory reporting elements as well as a standard complaint submission form that the hosting provider or website publisher must make available to the public. This document does not replace due process or other applicable law, and **when dealing with abuse the web hosting or publishing provider should always be engaged prior to contacting the registrar** because they have specialized tools and granular access to address the abuse occurring on their systems, as well as a direct relationship with the users of their services.

The registrar community hopes that this effort to provide education and guidance regarding the abuse complaint process will assist law enforcement, lawyers, and other complainants in submitting clear and well-formed complaints to the appropriate parties, resulting in a positive and proportionate response. The surest way to get a satisfactory response from a registrar regarding abuse is to provide the registrar with a court or administrative order, or some other mechanism of legal due process.

This is a living document, intended to create a collaborative conversation and body of work leading to more effective methods of reporting and handling abuse complaints within the Internet community. It is a platform for feedback and is not a finalized set of practices; registrars continue to set individual requirements and processes for handling abuse reports.

The first section of this document outlines general abuse reporting requirements, with additional requirements for specific types of abuse in subsequent sections. Finally, there are suggestions for how to contact the domain name registrar and identify the web hosting provider.

General abuse reporting requirements

Registrars are committed to investigating and addressing abuse complaints in a timely and reasonable manner. However, registrar compliance teams often receive complaints that do not contain the necessary information to allow them to take action.

The list of requirements below is for complaints across all types of abuse. **Complainants should provide as much of the requested information as possible to facilitate efficient handling by the registrar and incomplete complaints may not result in investigation**. Registrars will be more able to respond effectively to an abuse complaint when presented with thorough, relevant information.

Where the issue occurred

- Domain name(s) being complained about, ‘defanged’ if possible
- Specific URLs or subdomains within the domain where the abuse is occurring, if applicable
- Webhost, if known

As a best practice, domains and URLs should be provided in a “de-fanged” form, meaning they are adjusted such that the website address is clear but the link cannot be inadvertently followed. This is to ensure that the recipient does not accidentally click through and receive the malware, view the abusive content, etc. For example, the URL http://example.com could be changed to

hXXp://example[.]com. A person reviewing the request can easily identify the domain in question while there is no risk of unintentionally following the link.

What happened

- Thoroughly outline the situation and describe the harm occurring
    - Indicate steps necessary to replicate the abuse
- Provide information about the context and severity of the abuse, and any related evidence
    - If possible, include relevant and readable screenshots and/or links to information supporting the abuse claim as well as links providing direct evidence of the abuse
- If possible, provide the date and time when the abuse occurred, and the jurisdiction where the abuse occurred
- Describe the nature of the harm (e.g. physical, monetary), in relation to a person, client, business or group
- Describe the desired outcome from reporting the abuse
    - This could include things like suspension or nameserver change (so any related services do not work), transfer lock (so the registration service provider cannot be changed), and requests for confidentiality.
- Indicate if the complaint has already been sent to the web host, including a response if available
- Evidence of any previous contact with domain name owner regarding the complaint, and any responses, if applicable
- If known, the age, or how long the domain has been registered for

Who the reporter is

- Complete contact details for the reporter
- Status as a representative of a government or law-enforcement agency, if applicable
- Willingness to indemnify the registrar for any action taken, if applicable

If a registrar cannot determine what abuse is taking place, cannot verify or confirm the abuse, or if the activities fall outside the registrar's abuse policy, the registrar will be unlikely to take action. Also, incomplete or misdirected complaints burden registrar abuse teams, resulting in slower response times to actionable complaints. **Following these guidelines helps registrars more effectively investigate and respond to abuse complaints.**

ICANN | RrSG
Registrar Stakeholder Group

Type-specific abuse reporting requirements

Phishing, spam & malware

Many online security threats are the result of a malicious actor accessing a legitimate domain registrant's web hosting account, affecting a single page or entire website hosted on the domain name, email at that domain, or other related resources. The registrant or hosting account holder may have no knowledge of the abuse taking place using their domain name.

Registrars may be unable to take action on a reported abuse if they are not also the hosting provider for the site in question, unless the existence of abuse can be validated internally or through a trusted source. Registrars will typically only be able to take action on a spam message when it is used as a delivery mechanism for a different type of abuse, such as phishing, or if there is clear evidence of financial fraud used in conjunction with the registration of the domain

Additional complaint requirements for phishing

- The domain name, brand or business the phish is mimicking
- If possible, an example phish email, including the full email header information

Additional complaint requirements for spam

- A copy of a spam email, including the full email header information

Additional complaint requirements malware

- Evidence of the distribution of malware

Trademark infringement

Trademark infringement in domain names

If the domain name itself infringes on a registered trademark, the most effective course of action is the Uniform Domain-Name Dispute Resolution Policy ("UDRP"). When a trademark infringement complaint is sent to the registrar of record outside of the UDRP process, the registrar will in most cases direct the complainant to file a UDRP complaint. Some registrars may also forward the complaint to the domain owner, allowing them to address the complaint directly with the complainant. In order for any action to be taken on a domain, the registrar of

record in most cases must be presented with a valid court order or have the consent of the registrant.

The Uniform Rapid Suspension ("URS") process offers a lower-cost, faster path to relief for trademark owners experiencing clear-cut cases of infringement. While registrars are not a part of the URS process, registrars are aware of URS proceedings and may in some cases recommend that the registrant use the URS process to report a trademark-infringing domain.

Trademark infringement in website content

Registrars are a poor venue for a website content trademark infringement complaint as they typically do not provide or control the hosted content (unless the registrar is also the hosting provider) and thus cannot target specific content on a website; instead, **the complainant should contact the web host or otherwise follow legal due process.** Domain registrars cannot adjudicate legal disputes and will most likely not take action against the domain based on a content complaint unless it passed through approved ICANN arbitration procedures (i.e., UDRP and URS) or is accompanied by a valid court order. In addition to complying with local law requirements for reporting trademark infringement, following the recommendations above in 'General Abuse Reporting Requirements' will assist a registrar in investigating the complaint and encourage a timely response. While trademark issues found within content are generally inappropriate to resolve at a Registrar, submissions should include the following information.

Additional complaint requirements

- Evidence that the complainant is the trademark holder, or an agent of the trademark holder
- Reference to the law under which the trademark abuse is alleged

Copyright infringement

As with trademark infringement, **if copyright infringement occurs within the registered domain itself then a complaint should be directed to the registrar, while concerns about hosted content should be communicated to the web hosting provider.** Some countries have enacted legislation that places obligations on hosting companies, website publishers, and other service providers who have control of website content to process copyright infringement complaints in a certain manner. These laws can affect the requirements or processes established by the registrar for handling copyright complaints. That said, in addition to complying with local law requirements for reporting copyright infringement, utilizing the recommendations discussed above in 'General Abuse Reporting Requirements' will assist a registrar in investigating the complaint.

Additional complaint requirements

- Evidence that the complainant is the rights holder, or an agent of the rights holder
- Reference to the law under which the copyright abuse is alleged

Child abuse & child sexual exploitation material

Registrars take complaints of child abuse or sexual exploitation material very seriously, but are not able to review allegations of child abuse imagery as accessing such content may put the registrar in violation of applicable laws. As such, **do not send examples of child abuse or child sexual exploitation material to a registrar. Instead, all complaints about child abuse material must be sent to the appropriate national authority,** such as the National Center for Missing and Exploited Children (NCMEC) in the United States or the Internet Watch Foundation (IWF) in the UK. The registrar will take action on the relevant domain upon direction from the national authority.

Additional complaint requirements

- Do **not** send examples to the registrar
- All concerns about child abuse or exploitation material must be sent to the appropriate national authority

How to submit abuse reports

First, complainants should ensure they have correctly identified the Registrar of record for the domain in question. This can be done using a Whois lookup, either on the Registrar's website, or via a generic service like https://lookup.icann.org.

Complaints are often best submitted via the Registrar's website, which may have a submission form ensuring appropriate information is captured. Complaints may also be submitted to the Abuse contact listed in the results of the Whois lookup.

Nameserver information can often be used to identify a web hosting provider, so that a complaint can be submitted to them. For the relevant domain, do a Whois lookup and find the Nameserver information; then go to the domain name found in the Nameserver hostname or do a Whois lookup on that domain itself to identify the service provider. There are some cases where the Nameserver information does not identify the hosting provider (eg where a reverse

proxy service is being used) or lead to the abusive DNS resource, but Nameservers are typically a good starting point.

Be sure to provide all the information described in the sections above when submitting an abuse report to a registrar or web hosting provider.