

Change of Registrant (COR)

TPR Group 1(b): Part II

Meeting #110



Contractual Compliance speaker - Holida Yanik

Overview of Transfer Complaint metrics

(June 2018 - October 2023)

Change of Registrant - Process (revised)

Revised following TPR WG Meeting #109

COR Process (revised)

To complete the COR process, the Registrar must do all of the following:

1. **Confirm** the domain name is eligible for a Change of Registrant (~~Transfer Policy~~, Section II.B)
 - ~~The Registrar must deny a COR request if the COR was not requested properly authorized by the Prior Registrant and the New Registrant (or their Designated Agent).~~
 - ~~A Registrar must deny a COR request if there is evidence of (a) fraud or (b) the domain presents an active DNS Security Threat as defined here: <https://www.icann.org/dns-security-threat>.~~
1. **Send** a notification to the Prior Registrant and the New Registrant, informing them of the Change of Registrant request
 - The Registrar must inform the New Registrant (or its Designated Agent) that the New Registrant must enter into a registration agreement with the Registrar.
1. **Process** the Change of Registrant without undue delay, no longer than one calendar day (24 hours) of providing notification to both parties.
2. **Send** a notification to the Prior Registrant and New Registrant before or within one calendar day (24 hours) of the completion of the Change of Registrant.

The notification must:

 - explain the request that was received and list the domain(s) in question
 - include contact information for questions
 - **Additional requirements TBD**

★ Is it necessary to send two sets of COR notifications (upon COR request + COR completion, just COR completion, or either)?

COR Process (revised)

Step 5(?): If the New Registrant or Prior Registrant contacts the Registrar, claiming that they did NOT request the Change of Registrant...

Option 1: The Transfer Policy should not require anything more than the provision of contact information in the notification(s), allowing Registrars (or their resellers) to address reports of improper CORs as they see fit

Option 2: The Transfer Policy should require Registrars (or their resellers) to address or respond to reports of improper CORs

Option 3: The Transfer Policy should require Registrars (or their resellers) to have a dispute mechanism/process through which the Prior/New Registrant can challenge or correct an improper COR.

Option 4: Other?

Example Scenarios to consider:

- RNH John Doe updated his email address, but there is a **typo** and he wants to fix it.
- RNH Jane Doe's email was **hacked** and someone initiated a change of registrant without her knowledge.
- The **Privacy/Proxy** provider updated their anonymized email and the RNH James Doe wants to change it to his own information.
- The **Designated Agent** initiated a change of registrant and the RNH Jill Doe wants to change it to her own information.

COR + Registrar Transfer

What should happen when a COR is followed by an inter-Registrar transfer request?

COR + Registrar Transfer

With the removal of the 60-day inter-registrar lock that normally follows a COR:

If a Change of Registrant occurs and is then followed by a TAC request from the New Registrant...

Option 1: No special requirements are necessary. The TAC can be provided immediately upon the registrant's request or otherwise within 5 calendar days.

Option 2: Before issuing the TAC, the Registrar must send a notification to the registrant informing them of the TAC request and recent COR.

Option 3: The TAC would be provided within 5 calendar days ONLY if a recent change to the registrant's/account holder's information is successfully verified (per the RAA [Whois Accuracy Program Specification](#)).

Option 4: The TAC would be provided within 5 calendar days ONLY if no objection from the New or Prior Registrant is received during that time (i.e. a multi-day waiting period to transfer, when preceded by a COR).

Option 5: The Registrar must offer the RNH an OPT-IN option for added protections, such as a longer waiting period before the TAC is revealed following a COR, or multi-factor authentication.

Option 6: Other?

Appendix: Whois Accuracy Program Specification

Whois Accuracy Program Specification

Within 15 days of any change in the Registered Name Holder, the Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:

Validate:

- the presence of data for all required fields (RAA Subsection 3.3.1) are in a proper format for the applicable country/territory.
- that all email addresses are in the proper format
- that telephone numbers are in the proper format for international telephone numbers
- that postal addresses are in a proper format for the applicable country or territory
- that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country/territory.

Verify:

- the **email address** of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or
- the **telephone number** of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to them via web, email or postal mail.

Whois Accuracy Program Specification

If the Registrar does not receive an affirmative response from the Registered Name Holder, the Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information.

If the Registrar does not receive an affirmative response from the Account Holder¹, the Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

The Registrar is NOT required to perform the validation and verification procedures if the Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.

HOWEVER, if the Registrar has any information suggesting that the contact information specified is INCORRECT (such as Registrar receiving a bounced email notification), the Registrar must verify or re-verify, as applicable, the email address(es).

★ **Does the verification of RNH email and phone number already provide sufficient security regarding COR?**