FAQ: Registrant Domain Name Compliance Escalation and Suspension Policy

Trust and security are the bedrock of the value proposition for .BANK/.INSURANCE, and non-compliance with the mandatory Security Requirements (see more below) poses significant business and reputation risks for Registrants and fTLD Registry Services ("fTLD"). As such, fTLD's Advisory Council and its Board of Directors approved the **Registrant Domain Name Compliance Escalation and Suspension Policy** (the "Policy") to ensure a consistent approach to compliance actions for Registrants who fail to remediate their security vulnerabilities (i.e., compliance findings) within the time frames specified in the Policy.

Where can the Policy be found?

The Policy for .BANK is accessible here: https://www.register.bank/policies/ and for .INSURANCE here: https://www.register.insurance/policies/.

Where can the Security Requirements be found?

The Security Requirements for .BANK are available here: https://www.register.bank/securityrequirements/ and for .INSURANCE here: https://www.register.insurance/securityrequirements/.

Who is affected by this Policy?

.BANK/.INSURANCE domains in DNS that have failures (i.e., aren't compliant with one or more Security Requirements) that persist for more than 30 days.

When does the Policy go into effect?

The Policy implementation effective date is January 1, 2023.

What does it mean?

To ensure a consistent approach to compliance, fTLD will initiate compliance escalation notifications to the Registrant, with copy to the verification contact, and Registrar, for

domains that remain out of compliance with one or more Security Requirements, in accordance with the Escalation Process detailed in section 4 of the Policy.

What happens if a compliance failure is not resolved?

As outlined in the Policy, either the Registrar or fTLD will place the domain in a "hold" status and with this it no longer appears in the DNS, which means its websites and email will no longer function.

Who should I contact with questions?

For compliance questions, write to: compliance@fTLD.com. For your domain account or related questions for managing your domain's DNS, contact your Registrar. If you have any other questions, write to compliance@fTLD.com.

How do you know when your domain(s) are in or out of compliance?

If you are not receiving compliance notifications from compliance@fTLD.com to the Registrant Email for your .BANK/.INSURANCE domain(s), then you do not have any failures to remediate. If you wish to confirm your compliance status, you may write to: compliance@fTLD.com and identify the domain(s) in your email request.

What should I do if my domain is a defensive registration only?

If your domain is only intended for defensive purposes at this time, and you receive a compliance notification from fTLD, please contact us at compliance@fTLD.com and we can apply a serverHold status (no web/email) to exclude your domain from being subject to compliance security monitoring.

What's the difference between compliance warning notifications and compliance failures?

Compliance warnings are vulnerabilities we've identified and that we recommend the Registrant take action to resolve but are not mandatory and are therefore not a subject of this Policy. Failures must be addressed to remain compliant and to continue using your domain(s).

What if I need technical assistance with remediating the compliance failures?

If your Registrar provides technical services for your domain(s), you should first contact them. fTLD also provides information about vendors that can assist you in complying with the Security Requirements for .BANK at: https://www.register.bank/third-party-provider-program/ and .INSURANCE at: https://www.register.insurance/third-party-provider-program/. When in doubt, ask fTLD for assistance: compliance@ftld.com.