Frequently Asked Questions (FAQ) about Modifications to the Security Requirements
April 24, 2017

What are the Security Requirements?

fTLD Registry Services (fTLD) takes a proactive approach to working with the global financial services community to enhance trust in the online financial system. To accomplish this, fTLD employs robust consumer protection safeguards that include obligations for fTLD, its registrars and registrants to implement important Security Requirements (the "Requirements") designed to protect the integrity of fTLD's domains and to mitigate malicious activities such as cybersquatting, spoofing, phishing, data tampering and website misdirection.

fTLD's Requirements were initially developed in 2011 by its community-based Security Requirements Working Group (SRWG), an open working group comprised of volunteers with expertise in financial services, fintech and cybersecurity. The SRWG reviews the Requirements periodically and may recommend updates to address the evolving threat landscape of the financial services sector and emerging technologies designed to protect banks, insurance providers and distributors and the consumers they serve.

Consistent with fTLD's commitment to periodically review the Requirements, the SRWG undertook a recent assessment, and recommended several modifications to them that were approved by fTLD's Board of Directors on March 23, 2017.

The purpose of this FAQ is to detail the modifications to the Requirements. For reference purposes, .BANK/.INSURANCE domain names are referred to as in-zone and any other domain name is out-of-zone. For transparency, fTLD has provided a redline of the changes from the 2016 version to the new 2017 version here and the new Requirements here.

What are the modifications to the Security Requirements?

1. Requirement #27 is modified to specify that DNS Resource Records (e.g., CNAME, DNAME, MX) may be used to alias to out-of-zone domains and are subject to requirement #23, DNSSEC, by January 1, 2018, and requirements #25 and #29 (i.e., TLS encryption at the relevant version).

2. Requirement #29 is modified to differentiate Transport Layer Security (TLS) services to include: web connections, server-to-server email and other services (e.g., FTP, POP3, iMAP) as follows (and defined in requirement #29):

    a. **Web connections:** TLS v1.1 or greater should be maintained. TLS v1.0 may be used to serve educational information about the importance of browser hygiene and provide guidance about how to update a browser. Registrants should communicate to customers/visitors to their websites a specific date when access to their websites using TLS v1.0 will no longer be possible.

    b. **Server-to-Server Email:** For domains sending or receiving email, TLS v1.1 or greater must be offered at the highest priority. However, when exchanging mail with out-of-zone domains earlier versions of TLS/SSL are permitted, including, as the lowest priority, defaulting to unencrypted email when it is not possible to provide encryption.

    c. **Other services:** TLS v1.1 or greater should be used but TLS v1.0 does not need to be disabled at this time.

The TLS requirement will be revisited in Q1 2018 when other industry work on this topic may be nearing completion, which may provide support for additional changes to it.

3. Requirement #30 is modified to specify that redirection to out-of-zone domains must be made from the HTTPS version of an in-zone domain. Out-of-zone domains operated by third-party providers are not subject to compliance with the Requirements. With this change the integrity of fTLD's operations of its zones is preserved and what registrants choose to do with customers/visitors to their website outside of the .BANK/.INSURANCE zone is a risk-based business decision they will make for themselves.

4. Annex A has been eliminated based on the following:
    a. Hosted Email Solutions: As fTLD requires DMARC and SPF and/or DKIM for in-zone domains, registrants have control over who sends email on their behalf either directly as with an email marketing service provider or indirectly such as with Google and Outlook 365 whose platforms provide email services for their customers.
    b. Content Delivery Networks: As CDN services are generally deployed using a CNAME, the modification noted above in #1 applies to them.
    c. Security and Fraud Services: As these services are generally deployed in a manner that does not impact the customer's experience accessing a registrant's website, there is no basis for requiring compliance with the Requirements by out-of-zone domains.
    d. Aliasing to Legacy Domains: This is covered above in #1.
5. Other non-material revisions were made to clarify and streamline the Security Requirements.

What domains are in-scope for the Security Requirements?

All second-level, in-zone domains and subdomains remain in-scope. Further, out-of-zone domains that provide services to in-zone domains via DNS Resource Records such as CNAME and MX are considered in-scope, and must comply with the DNSSEC and TLS requirements as described in requirement #27.

When do third-party providers that alias using DNS Resource Records need to comply with DNSSEC?

The date for requirement #23 (i.e., DNSSEC) is January 1, 2018.

What happens to my domain if I do not comply with the Security Requirements?

fTLD is monitoring all in-scope domain names for compliance with the relevant Requirements. fTLD will notify registrars and registrants of domain names that are not compliant. Failure of the registrar/registrant to provide a timely response to fTLD and to implement a mutually-agreeable remediation plan may result in the domain name being removed from the .BANK/.INSURANCE zone (i.e., it will not resolve on the internet), or other significant actions such as domain name revocation.

How do modifications to the Security Requirements effect the Guides to Leveraging an fTLD Domain?

The Guides available on fTLD's websites account for the modifications to the Security Requirements.

Who should I contact with questions about the Security Requirements?

Questions should be submitted to fTLD@fTLD.com and include as much detail as possible to ensure a thorough and complete response.