As per our email to you in December 2020 and associated announcements on our websites of December 18, 2020 for .BANK (and for .INSURANCE here) and to Registrants, fTLD has modified the Security Requirements to require Registrants who have implemented DNSSEC for their .BANK/.INSURANCE domain(s) to ensure they use strong cryptographic algorithms (i.e., exclude SHA-1 digest in Delegation Signer (DS), CDS, and SSHFP records; and RSASHA1 for DNSKEY and CDNSKEY records).

We understand that some DNS providers support SHA-1 in DS resource records to provide compatibility for older name servers. However, upon consultation with our security monitoring vendor and in-house security adviser, we do not find there to be sufficient rationale to support this use case, especially when considering RFC-8624 has stated clearly that no new SHA-1 keys should be created and furthermore, it has been more than 10 years since the deprecation of SHA-1 a cryptographic hash function (and 8 years for use in digital signatures) so use this far beyond its deprecation is no longer warranted.