FAQ: Public Suffix Domain (PSD) DMARC (Domain-based Message Authentication, Reporting and Conformance)

Trust and security are the bedrock of .BANK/.INSURANCE. To build on this, fTLD Registry Services ("fTLD") sponsored development of a new extension to DMARC called PSD DMARC and will deploy it for .BANK and .INSURANCE on November 15, 2023. While .BANK and .INSURANCE have a pristine reputation, we want to take proactive measures to keep it that way for your benefit. PSD DMARC provides .BANK and .INSURANCE with protection from common types of fraudulent email attacks thereby mitigating reputation and other damaging risks associated with them. .BANK and .INSURANCE are the first non-governmental Top-Level Domains (TLDs) to provide this capability.

All .BANK and .INSURANCE domains are covered by the new PSD DMARC security feature when it is added. No action is required by domain customers to enable this new feature.

How does PSD DMARC work?

When mail service providers (MSPs) such as Google and Microsoft query a domain name for its DMARC record, if one is found the DMARC record is followed. In contrast, if an MSP's query does not find a DMARC record for a domain name, there's a second query at the TLD level and starting November 15, 2023, for .BANK/.INSURANCE they would find the PSD DMARC record and can follow it.

What changes do I need to make for my .BANK/.INSURANCE registered domain(s) due to PSD DMARC?

None. This new extension is automatically implemented for you by fTLD to further protect .BANK/.INSURANCE from certain forms of email-based abuse.

How does PSD DMARC affect my .BANK/.INSURANCE registered domain(s)?

For registered domains published in the .BANK/.INSURANCE zone (i.e., a live, parked, redirecting, or otherwise technically resolving domain):

- If there's a DMARC record currently in place, there is no impact to your email authentication policy, just the added phishing and spamming protection provided by the new PSD DMARC extension. In the event of any temporary issues which prevent registered domains from serving their domain's DMARC record, PSD DMARC provides a backstop policy to improve the overall consistency of DMARC protections.

- If there's not a DMARC record, PSD DMARC provides DMARC policy information to email receivers to prompt them to block or reject fraudulent emails from being delivered.

For registered domains not published in the .BANK/.INSURANCE zone (e.g., some defensive registrations), PSD DMARC provides DMARC policy information to email receivers to prompt them to block or reject fraudulent emails from being delivered.

What data will be collected due to PSD DMARC?

PSD DMARC has no effect on DMARC feedback reporting for registered domains (published in the .BANK/.INSURANCE zone) that have a DMARC record. fTLD may receive aggregate feedback reports for registered domains not published in the .BANK/.INSURANCE zone and non-existent domains (i.e., NXDOMAINs).

How is data collected for PSD DMARC going to be used?

fTLD will use PSD DMARC aggregate data for detecting abuse or potential threats, enforcing compliance with the DMARC Security Requirement, and enhancing the overall security and stability of the .BANK/.INSURANCE TLDs.

Where can I learn more about PSD DMARC?

Technical details of PSD DMARC can be found in the Internet Engineering Task Force's (IETF's) Request For Comment (RFC) 9091 found here:

https://www.rfc-editor.org/info/rfc9091

Additional information is available from:

https://psddmarc.org/

When will fTLD publish PSD DMARC records?

fTLD will publish PSD DMARC records on November 15, 2023.

What is fTLD's DMARC Security Requirement?

The requirement for .BANK is available here: https://www.register.bank/securityrequirements/ and for .INSURANCE here: https://www.register.insurance/securityrequirements/. Detailed information is accessible here: https://go.ftld.com/dmarc-implementation.

Who should I contact with questions?

Please write to: compliance@fTLD.com.