September 16. 2013

Mr. Fadi Chehade, President, CEO of ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Re: Proposal to Mitigate Name Collision Risks

Dear Mr. Chehade,

In response to the call for comments regarding proposed efforts to mitigate potential impact resulting from name collisions as New gTLDs are delegated into the root zone, the Online Trust Alliance is submitting the following comments.

As an independent non-profit, OTA is a global organization addressing the end-to-end trust issues and challenges faced by consumers, online merchants and online financial services companies. A primary goal of OTA is to increase consumer protection and transparency and ensure consumer control over their data, online activities and transactions, thereby enhancing online trust and confidence. OTA represents a wide variety of constituencies ranging from leading interactive marketers, government organizations, domain registrars, advertisers, and technology and solution providers to privacy advocates, academics, and merchant card processors.

Our diversity and autonomy fosters the development of balanced recommendations and policies which are in the best interest of the consumer and we are not beholden to any single business sector. As a global organization, OTA has members in Australia, Canada, Demark, England, Germany, Mexico, Netherlands, Romania, Singapore, Switzerland, Taiwan and the United States.

Respectfully,

Craig Spiezle
Executive Director & President
Online Trust Alliance
https://otalliance.org
+1 425-455-7400

Responses to Proposal to Mitigate Name Collision Risks

There's no question that domain collisions are both frequent and alarmingly widespread: the amount "leakage" — DNS queries for domain names based on the new gtlds that don't exist — are only the tip of a lethal iceberg that threatens all kinds of businesses. The home network, the smallest shop in Nairobi, the regional grocery store in Australia, and the largest global enterprise, are all for a big and potentially devastating surprise. When businesses fall victim to domain name collisions, their IT operations are severely disrupted at best, and completely disabled in the most likely scenario.

Large enterprises have thousands of desktop computers and mobile devices that depend on domains whose resolution will soon no longer be predictable, resolving to different servers operating in completely different organizations, depending on where the DNS query was issued. Because of DNS caching, both on client devices and servers, the problems may magically appear and go away for no apparent reason.

The large majority of servers accessed through these no-longer-reliable domains are used for mission critical services like authentication, databases, email, and collaboration. A single domain collision has the potential to bring down the entire IT organization of an enterprise, including thousands of desktop computers and mobile devices that can no longer access mission critical servers. Many internal line-of-business applications were written at a time when nobody imagined that the internal domains their business depends on would one day be up for grabs.

For small businesses the problem will be equally devastating, at the very least. Most have no internal IT resources or expertise and have to rely on third party service providers and hosters who they have limited experience with their systems. Because of the potentially intermittent nature of the problem (due to DNS caching) they may spend months wasting valuable time before even realizing what's happening.

Hiring external consultants to fix these problems is both expensive and time-consuming, and especially costly when the mission-critical systems their business runs on are no longer available. These small and medium businesses are just trying to run their operations and have no knowledge of the issues, nor time to get involved. They are overwhelmed with the technology and the overhead of running a business.

The most troubling aspect of domain collisions is the staggering cost to fix them. For enterprises, even the task of making an inventory of all devices, configurations, and applications that depend on domains that used to work flawlessly for years, is enormous. Updating the configuration of these devices is both tedious and risky, and enterprise desktop configuration management tools are likely to only be able to address part of the issue. Small businesses, which don't have enterprise client management tools, will have to hire (expensive) outside consultants to manually change each configuration, after they finally identified the cause of the problem.

Most devastating are internal software applications that depends on colliding domains. Many applications were built years ago using development tools and libraries that are no longer available and no longer supported. The developers with the competence to fix these applications have long ago moved onto other projects or even left the company. These applications are effectively impossible to fix and will suddenly become unreliable, failing and/or sharing confidential information with servers outside the organization.

This is not just an issue with server-side code. There are unimaginable numbers of client-side EXEs in languages like C, Visual Basic, PowerBuilder, etc. But Visual Basic 6 support ended in 2008; PowerBuilder support ended in 2011. Many of the plug-in components that these applications depend on are no longer sold and supported.

At this time we do not have any data on the breadth and costs/challenges to fix and recompile. ICANN should undertake further study on this potentially serious and expensive remediation issue. This would include outreach to those entities querying a new TLD, asking how they intend to remediate and whether they have the programming components and compilers are still available.

As ICANN proceeds with excitement about the thousands of new domains that will soon be available for businesses, let's not forget the millions of businesses that may very well be devastated by a problem they are not even aware of today.

We owe it to these home users and businesses of all sizes and in all countries, to proceed with caution, raise awareness, and provide a clear transition plan that helps them definitively address this issue proactively.