

**Rec. 24**

1. Safeguards for Sensitive and Regulated Strings

The GAC identified a nonexhaustive group of nearly 200 strings (Category 1) that raised consumer protection concerns, contained sensitive strings, or strings in regulated markets and advised that five safeguards should apply to these Category 1 strings. The GAC explained that strings linked to “regulated or professional sectors should operate in a way that is consistent with applicable laws” and observed that the identified strings were “likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm<sup>1</sup>.” During implementation, however, ICANN included only a subset of these GAC-identified strings within the Category 1 safeguard protections<sup>2</sup>. In addition, during implementation, ICANN included only three of the five GAC-recommended safeguards to its selected subset of Category 1 strings in regulated markets<sup>3</sup>.

As implemented, these safeguards took the form of downstream contract requirements contained in the Public Interest Commitments Specification of the Registry Agreement. Specifically, the safeguards required registry operators to obligate registrars vis-à-vis the Registry-Registrar Agreement to include certain provisions in their Registration Agreements with registrants.

The requirements for sensitive strings and those in regulated markets included provisions requiring registrants to comply with all applicable laws<sup>4</sup>. Another provision emphasized that this obligation includes “those [laws] that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures<sup>5</sup>.” Furthermore, specific provisions detailed requirements for registrants handling sensitive information, such as health or financial data, to “implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law<sup>6</sup>.”

<sup>1</sup> ICANN GAC (11 April 2013), “Beijing Communiqué,” p. 8.

<sup>2</sup> Ibid. Compare the Beijing Communiqué with ICANN’s implementation framework for GAC Category 1 implementation advice: ICANN, “GAC Advice: Category 1 Safeguards,” accessed 7 February 2017, <https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards>; and ICANN New gTLD Program Committee (NGPC) (5 February 2014), GAC Category 1 Safeguards: Annex 2: ICANN NGPC Resolution No. 2014.02.05.NG01, accessed 7 February 2017, <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>; October 29, 2013 letter Crocker to GAC Chair; September 2, 2014 letter Crocker to GAC Chair; and June 23, 2015 Crocker to GAC Chair.

<sup>3</sup> Ibid. See also October 29, 2013 letter Crocker to GAC Chair; September 2, 2014 letter Crocker to GAC Chair.

<sup>4</sup> ICANN, “Registry Agreement,” Specification 11, 3(f).

<sup>5</sup> ICANN, “GAC Advice: Category 1 Safeguards” and ICANN NGPC, Category 1 Safeguards.

<sup>6</sup> Ibid.

**Formatted:** No bullets or numbering  
**Formatted:** Font:Times New Roman, Bold

**Formatted:** Font:11 pt  
**Deleted:** Communique  
**Formatted:** Font:11 pt  
**Formatted:** Font:11 pt  
**Formatted:** Font:11 pt  
**Deleted:** Communique  
**Formatted:** Font:11 pt  
**Formatted:** Default Paragraph Font, Font:11 pt  
**Formatted:** Default Paragraph Font, Font:11 pt

It is difficult to determine whether these safeguards have been the subject of complaints to ICANN contract compliance because the categories of complaints identified in ICANN’s Compliance Reports do not provide this level of detail. That is, the reported ICANN complaint categories for registries and registrars such as “PIC” (Public Interest Commitments) or “Abuse,” do not contain sufficiently specific information to correlate complaints with specific safeguards. However, the ICANN Global Consumer Surveys noted much lower comfort levels when consumer end users were asked about providing sensitive information (including financial and health information) to new gTLDs as compared to legacy gTLDs.<sup>7</sup> Moreover, another survey on trust in the internet reflected the public’s increasing concerns regarding stolen credit card/financial information; online security; protection and security of credit card and personal information.<sup>8</sup> ICANN Compliance does report that it proactively monitored compliance with Specification 11, paragraph 3a that includes the obligation for downstream contracts to include language requiring compliance with applicable laws, and determined that there was 99% compliance with this provision<sup>9</sup>.

2. Recommendations

**Rec. 23 is not the topic of my revision:**

**Recommendation 24.** Initiate discussions with relevant stakeholders to determine what best practices are being implemented to offer reasonable and appropriate security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information. Such a discussion could include identifying what falls within the categories of “sensitive health and financial information” and what metrics could be used to measure compliance with this safeguard.

**Rationale/related findings:** The lack of publicly available information about whether ICANN Contractual Compliance has received complaints related to the implemented Category 1 safeguards, and lack of a common framework to define sensitive information, make it difficult to assess what impact this safeguard has had on mitigating risks to the public. However, protection of sensitive information, particularly sensitive financial and health information is a high priority for Internet users. As a result, this recommendation aims at improving both complaint data regarding these issues and encouraging communications about best practices on how to protect these sensitive categories of information.

**Measures of Success:** This Recommendation would be successful if relevant stakeholders, to include new gTLD registries and stakeholder groups representing the public interest, discuss what constitutes sensitive information and best practices regarding how to protect sensitive information. Such discussions could inform future policy in this area with a goal of increasing the public’s trust of new gTLDs.

<sup>7</sup> See *infra* pp. X-X, *Consumer Behavior that Indicates Trust* and accompanying footnotes.

<sup>8</sup> See NCC Group, *Trust in the Internet Survey* (2016), p. 2.

<sup>9</sup> ICANN (2015), *ICANN Contractual Compliance 2014 Annual Report*, p.13.

**Deleted: Recommendation 23.** Include more detailed information on the subject matter of complaints in ICANN publicly available compliance reports. Specifically, more precise data on the subject matter of complaints, particularly (1) what type of law violation is being complained of and (2) an indication of whether complaints relate to the protection of sensitive health or financial information, would assist future Review Teams in their assessment of these safeguards. **Note:** A general recommendation for further transparency regarding the subject matter of complaints received by ICANN Contractual Compliance is set forth in [Chapter V, Data-Driven Analysis: Recommendations for Additional Data Collection and Analysis](#)

**Formatted:** Font:14 pt, Bold

**Formatted:** Font:Italic

**Deleted:** constitutes

**Deleted:** and identify what constitutes “reasonable and appropriate security measures”

**Formatted:** Font:Bold

**Formatted:** Font:Not Bold

**Formatted:** Font:Not Italic

**Formatted:** Font:Not Italic

**Formatted:** Font:Italic

**Formatted:** Font:Not Italic

**Formatted:** Font:11 pt

**Formatted:** Font:11 pt, Italic

**Formatted:** Font:11 pt

**To:** ICANN organization

**Prerequisite or Priority Level:** High

**Consensus within Team:** Yes

**Formatted:** PleadingTitle