From the desk of
Jonathan Matkowsky, VP – IP & Brand Security

Writer's Direct Cell: Contact Information Redacted

VIA EMAIL <goran.marby@icann.org>, <cherine.chalaby@icann.org>

Mr. Göran Marby
ICANN President and CEO

Mr. Cherine Chalaby
Chair
ICANN Board

March 26, 2018

Request for Adequate Assurances Relating to WHOIS and GDPR

Dear Messrs. Marby and Chalaby:

As background, RiskIQ, Inc. ("RiskIQ") is a leader in digital threat management, providing comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than seventy five percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by tens of thousands of security analysts, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action to protect government, business, brand, and customers.

RiskIQ and other digital threat management professionals, such as the security and anti-abuse community, intellectual property professionals and their respective rightsholders, including our clients ("we" or "us"), rely on WHOIS data as an essential element in discovering, identifying, tracking and mitigating threats online. WHOIS data is used in conjunction with a number of other data points by RiskIQ as part of managed security services, and by our end-user security analysts, to protect our clients, their downstream customers and end-users, and ultimately, the Internet and public.

We are currently being damaged, including by our inability to plan, prepare and execute our clients' ongoing digital threat management, because ICANN has failed to timely[1] finalize an enforceable interim model that adequately provides access to WHOIS data. It is unrealistic to expect a major platform used by tens of thousands of security professionals to be adjusted last

[1] ICANN must act "with a speed that is responsive to the needs of the Internet as part of the decision-making process." ICANN Bylaws, § 1.2(b)(v).

minute, and the current interim model (the so-called "Calzone") is not finalized and makes unavailable huge swathes of critical data sets – far beyond what is required by GDPR. With only sixty days left, having a draft document reflecting "over-compliance" with GDPR is an egregious violation of ICANN consensus policies--unmistakenly undermining the stability and security operations of the Internet's unique identifier systems. Through such acts and omissions, ICANN has caused, is causing, and continues to cause damage to the openness, interoperability, resilience, security and stability of the DNS, which is not required by applicable law (including GDPR pursuant to *any* reasonable interpretation).

It is the ICANN Board's responsibility taking into account the urgency involved to have at least adopted and established a "Temporary Policy" to "maintain the stability or security of Registry Services or the DNS"[2] that can be relied on. This grossly negligent ICANN behavior is unconscionable in light of its Mission and Bylaws, and is a proximate cause of our injury being suffered. The draft interim draft model--particularly at this point--*is* a failure by ICANN to have carried out its Mission to ensure the stable and secure operation of the Internet's unique identifier systems through actions that facilitate the openness, interoperability, resilience, security and/or stability for the DNS, including policies relating to registry operations or registrars.

ICANN's inability to make certain WHOIS data available in the public data sets (with tiered-access for that which cannot be available under applicable law) harms us, particularly the corporate and government infrastructure we help protect, and the public-at-large. For instance, RiskIQ, just like all those similarly situated, has been, and continues to be left in a position where we are unable to adjust our platform in the most effective manner to detect, analyze, and mitigate threats within a GDPR framework because the datasets are in flux and already less reliably available. This is due to ICANN's lack of effective leadership described herein, causing vulnerabilities to critical infrastructure such as banking, healthcare, and other vital sectors the public depends on, which has created, and continues to create, an increasingly and unacceptably dangerous threat environment for commerce--from interstate to foreign and domestic.

ICANN is accountable to the Internet community for operating in accordance with its Articles of Incorporation and the Bylaws, including its Mission. We draw your attention to the March 15, 2018 **GAC Communiqué** – San Juan, Puerto Rico, particularly ***GAC Consensus Advice*** to the Board with respect to WHOIS and the GDPR, including the rationale for the Consensus Advice on pages 9-10 therein. If ICANN were to adopt the "Calzone" model or a substantially similar iteration that suffers from the same flaws, ICANN would be taking "an action that is not consistent with"[3] (*i.e.*, rejecting) GAC Advice. Under the ICANN Bylaws, GAC Consensus Advice may only be rejected by a vote of no less than 60% of the Board,[4] and the GAC and the Board are required to "then try in good faith, and in a timely and efficient manner, to find a mutually acceptable solution."[5] Under the circumstances as described herein, ICANN's obligation to be "timely and

[2] Registry Agreement, Specification 1, at ¶ 1.4.
[3] ICANN Bylaws, as amended, § 12.2(a)(x).
[4] *Id.*
[5] *Id.*

efficient" means that ICANN must immediately cure its acts and omissions that have caused, and continue to cause it to be in violation of the Bylaws.

Privacy is not an acceptable basis to deprecate security: there is no such thing as privacy without security.[6] We are dismayed to see how ICANN has been incapable of "prioritizing the facilitation of understanding and consensus between warring stakeholder groups" and rising to its Mission by having undertaken its greater obligations to the Internet as a whole. While we understand from the press that you may have requested enforcement forbearance from GDPR pending completion of an accreditation system, we have not been able to find any documents relating to this request. We need this information to try and help mitigate the damages that ICANN has, and continues to cause. We hereby formally request, therefore, that ICANN provide the following pursuant to ICANN's Document and Information Disclosure Policy ("DIDP")[7]:

> *All documents or correspondence in electronic or paper form referring or relating to enforcement forbearance from GDPR, specifically including policies, plans, and correspondence with DPAs or any other authorities and any responses thereto.*[8]

ICANN must have a means to compel the registrars and registry operators to provide access to WHOIS data to the extent allowed by applicable law, to participate in the tiered access model, and to cooperate with all efforts to provide these necessary services. We fear registrars are going to overly mask their data come May, and whether or not ICANN has come up with a model that is widely adopted, we must know that ICANN will be in a position to enforce its agreements with the Registries and Registrars consistent with applicable law.

It appears the ICANN Board has been deferring to "ICANN org" and letting senior staff make these decisions. The time has come for the Board to act immediately. As it stands, ICANN's Cookbook is too late in the game, and in any case would be an approved recipe for turning the open Internet into a Tor-like deep and dark net, unnecessarily hindering the efforts of digital threat management--whether that be targeting human capital, stealing intellectual property, or any other malicious cybercriminal-related activities. The Board needs to take swift and decisive action to ensure that, consistent with its Mission, its Bylaws, applicable law and GAC Advice, WHOIS data remains available to us.

For all the foregoing reasons, we respectfully request adequate assurances in writing **by no later than March 31, 2018**, that the interim model has been revised and effectuated in an enforceable

---

[6] Ironically, one of the threat categories being undermined that we detect, analyze and mitigate includes ***Privacy Interferences***. GDPR is supposed to *strengthen* privacy--not *undermine* it.

[7] https://www.icann.org/resources/pages/didp-2012-02-25-en

[8] ICANN's Bylaws require ICANN, its Board of Directors and its staff to act in an open, transparent and fair manner with integrity. ICANN Bylaws, 1.2(a).

manner, so that it is not "over-compliant" with GDPR[9] but protects data in accordance with applicable law, and includes an appropriate method of tiered access that will allow us to maintain the "stability and security" of the Internet.

Nothing contained herein is intended to waive any rights of RiskIQ or of any of its clients or other organizations that join in making this request, all of which are expressly reserved. We will continue to supplement the signatories of clients and organizations that have joined in making this request, and keep you advised.

Thank you in advance for your anticipated cooperation.

Very truly yours,

cc: GAC Public Safety Working Group, Co-Chairs
<didp@icann.org>
Gregory S. Shatan, Esq.

[9] For example, and without limiting the points raised by the GAC Consensus Advice, it must not subject the data of legal persons to data secrecy, and if the balancing analysis under GDPR does not in the end permit for the email addresses of natural persons to be in the public data set, then before you strip away the most important data element for this subset, it must first be replaced only by a pseudonymous substitute with parity across Whois databases.