~~18~~ Updated 26 August 2020

RE: CommuniGal Communication Ltd. (GalComm)

Derek A. Newman
Newman DuWors LLP
100 Wilshire Blvd., Suite 700
Santa Monica, CA 90401

Dear Mr. Newman,

Thank you for your letter of 21 July 2020. We appreciate that GalComm has shared the actions it has taken to investigate potential DNS security threats in domains identified in the report from Awake Security entitled "The Internet's New Arms Dealers: Malicious Domain Registrars."

As GalComm is aware, under the 2013 Registrar Accreditation Agreement, specifically section 3.18, registrars are obligated to have a published point of contact to which incidents of abuse can be reported and have a duty to investigate those reports. Failure to publish the point of contact or investigate reports of abuse can, when reported to ICANN and not remedied, lead to termination of the Registration Accreditation Agreement. ~~To date, Awake Security has not contacted ICANN or provided any information directly to ICANN regarding their report.~~[1]

Having not been informed of any concerns by Awake Security prior to publication of their report, the Security, Stability and Resiliency (SSR) team within ICANN's Office of the CTO conducted an analysis of GalComm's domain portfolios against well-respected reputation block lists (RBLs) after Awake Security's report was published. The SSR team was unable to corroborate the findings Awake Security presented and it does appear that Awake Security had an inaccurate picture of the total domains under management by GalComm. Based on the information we have been able to obtain to date, we have no reason to believe it appropriate for GalComm to be considered a "malicious domain registrar" as asserted by Awake Security. However, as noted in Awake Security's report, the malicious actors behind the domains in question may be utilizing detection evasion techniques. As such, our investigations continue, and we appreciate GalComm's cooperation and support of those investigations.

As we have done in the past, we continue to encourage all registrars to utilize respected RBLs as a resource to help identify potential DNS security threats within their portfolios and take appropriate action to mitigate those threats. As always, ICANN's Office of the CTO remains a resource to the registrar community and if further consultation is desired, the GDD account manager supporting GalComm can facilitate such engagement.

Thank you for providing additional background and the efforts to stay vigilant regarding potential DNS security threats within the GalComm domain portfolios.

Sincerely,

Russ Weinstein
Vice President, GDD Accounts and Services
Internet Corporation for Assigned Names and Numbers (ICANN)

[1] Correction: Awake Security contacted ICANN via their outside counsel on 6 August 2020. See letter from Weinstein to Woo https://www.icann.org/resources/pages/correspondence.