crowell moring

Annex 16.

crowell moring

7, Rue Joseph Stevens, B-1000 Brussels ▪ p+32 (0)2 282 40 82 ▪ f+32 (0)2 230 63 99

Our ref fpe/mne/
Your ref

Flip Petillion
Advocaat
Contact Information Redacted

June 5, 2015

By Email

ICANN
To the attention of:

Members of the ICANN Board
and

Mr Akram Atallah,
President, Global Domains Division

Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Dear Members of the ICANN Board of Directors and Mr Atallah,

Re: Recent Data Exposure Issues in the New gTLD Applicant and GDD portals

I am writing to you on behalf of Travel Reservations SRL (formerly, Despegar Online SRL), Donuts Inc. (and its subsidiary applicant Spring McCook, LLC), Famous Four Media Limited (and its subsidiary applicant dot Hotel Limited), Fegistry LLC, Minds+Machines Group Limited (formerly, Top Level Domain Holdings Limited), and Radix FZC (and its subsidiary applicant DotHotel Inc.).

My clients are all applicants for the .HOTEL gTLD and express their deep concern about a recent data exposure issue that occurred in the New gTLD Applicant and GDD portals. Specifically, the user credentials of one person (D. Krischenowski) were used to conduct over 60 searches that resulted in over 200 unauthorized access incidents across an unknown number of TLDs. In this way, sensitive and confidential business information concerning several of the .HOTEL applicants was obtained. This matter is of direct concern to my clients; the situation is all the more worrying as D. Krischenowski, the holder of the user credentials, is associated with competing TLD applicants, including a competing applicant for .HOTEL, HOTEL Top-Level-Domain s.a.r.l. ('HOTEL sarl'), to which priority status has been granted and which forms the subject of discussion in a pending Independent Review Process.

The limited information that has so far become available shows that the user was deliberately looking for sensitive and confidential business information concerning competing applicants.

Allocating a critical Internet resource to an applicant associated with fraudulent action is a serious risk to the public interest that requires appropriate action by ICANN.

My clients request full information concerning this data exposure issue and the actions that have been taken by ICANN to limit damages for the affected parties. In particular, I would ask you to provide me with the following information:

- What was the precise nature of the security issue?
- When did the security issue occur?
- How could the security issue occur?
- How could the security issue have been avoided?
- How was the security issue discovered?
- Who raised the security issue?
- How did the security issue come to ICANN's attention?
- What actions did ICANN take after being informed of the security issue?
- How does ICANN enforce the portal's terms and conditions in case of obvious breach?
- What are the concrete actions that ICANN undertook vis-à-vis D. Krischenowski?

Please also send me a copy of the terms and conditions to which D. Krischenowski agreed and of the correspondence with D. Krischenowski and his legal counsel. Needless to say that a mere statement by a legal counsel denying improper or unlawful action is an insufficient ground for ICANN to refrain from taking further action.

My clients ask for full transparency and appropriate measures by ICANN.

We appreciate your attention to and consideration of this matter.

Sincerely yours,

Flip Petillion

crowell moring

Annex 17.

Response to Documentary Information Disclosure Policy Request

To: Flip Petillion

Date: 5 July 2015

Re: Request No. 20150605-1

Thank you for your request dated 5 June 2015 (the "Request"), which was submitted pursuant to the Internet Corporation for Assigned Names and Numbers' (ICANN) Documentary Information Disclosure Policy (DIDP) on behalf of Travel Reservations SRL (formerly, Despegar Online SRL), Donuts, Inc. (and its subsidiary applicant Spring McCook, LLC), Minds + Machines Group Limited (formerly, Top Level Domain Holdings Limited) and Radix FZC (and its subsidiary applicant DotHotel Inc.). For reference, a copy of your Request is attached to the email forwarding this Response.

Items Requested

Your Request seeks the disclosure of the following information regarding the data exposure issue in the New gTLD Applicant and GDD (Global Domains Division) portals first reported on 1 March 2015:

1. What was the precise nature of the security issue?
2. When did the security issue occur?
3. How could the security issue occur?
4. How could the security issue have been avoided?
5. How was the security issue discovered?
6. Who raised the security issue?
7. How did the security issue come to ICANN's attention?
8. What actions did ICANN take after being informed of the security issue?
9. How does ICANN enforce the portal's terms and conditions in case of obvious breach?
10. What are the concrete actions that ICANN took vis-à-vis D. Krischenowski?

You also requested a copy of the terms and conditions to which D. Krischenowski agreed and the correspondence with D. Krischenowski and his legal counsel.

Response

ICANN's DIDP is limited to requests for documentary information already in existence within ICANN that is not publicly available. Simple requests for non-documentary information are not appropriate DIDP requests. Nevertheless, the majority of your questions (Items 1, 2, 3, 5, 6, 7, and 8) have been addressed by the public announcements and Q&A published on the New gTLD microsite and have been readdressed below. (*See* http://newgtlds.icann.org/en/announcements-and-media/announcement-01mar15-en, http://newgtlds.icann.org/en/announcements-and-media/announcement-02mar15-en, http://newgtlds.icann.org/en/announcements-and-media/announcement-2-02mar15-en, http://newgtlds.icann.org/en/announcements-and-media/announcement-30apr15-en, and http://newgtlds.icann.org/en/announcements-and-media/announcement-27may15-en.)

On 27 February 2015, ICANN received notice of a potential security issue affecting the New gTLD Applicant and GDD (Global Domains Division) portals. Upon notification, ICANN confirmed the reported issue and immediately took the portals offline to address the issue. (*See* https://www.icann.org/news/announcement-2015-03-01-en.) Under certain circumstances, an authenticated portal user could potentially view data of, or related to, other users. Access to, and data in, these portals is limited to New gTLD Program applicants and New gTLD registry operators. These portals contain information from applicants to ICANN's New gTLD Program and new gTLD registry operators. No other systems were affected. The portals' configuration was updated to the address the issue and the portals were restored on 2 March 2015. (*See* https://www.icann.org/news/announcement-3-2015-03-02-en.)

ICANN conducted an in depth forensic investigation into whether any data was exposed to an unauthorized user. Two consulting firms reviewed and analyzed all log data going back to the activation of the New gTLD Applicant portal on 17 April 2013 and the activation of the GDD portal on 17 March 2014. The results of the investigation indicate that the portal users were able to view data that was not their own. Based on the investigation to date, the unauthorized access resulted from advanced searches conducted using the login credentials of 17 users, which exposed 330 advanced search result records, pertaining to 96 applicants and 21 registry operators. These records may have included attachment(s). These advanced searches occurred during 36 user sessions out of a total of nearly 595,000 user sessions since April 2013. Based on the information that ICANN has collected to date, our investigation leads us to believe that over 60 searches, resulting in the unauthorized access of more than 200 records, were conducted using a limited set of user credentials. The remaining user credentials, representing the majority of users who viewed data, were either used to:

- Access information pertaining to another user through mere inadvertence and the users do not appear to have acted intentionally to obtain such information. These users have all confirmed that they either did not use or were not aware of having access to the information. Also, they have all confirmed that they will not use any such information for any purpose or convey it to any third party; or

- Access information of an organization with which they were affiliated. At the time of the access, they may not have been designated by that organization as an authorized user to access the information.

(*See* https://www.icann.org/news/announcement-2015-05-27-en.)

Following the conclusion of the first phase of its forensics investigation, ICANN contacted the users who appear to have viewed information that was not their own and required that they provide an explanation of their activity. ICANN also asked them to certify that they will delete or destroy all information obtained and to certify that they have not and will not use the data or convey it to any third party. (*See* https://www.icann.org/news/announcement-2015-04-30-en.) ICANN also informed the parties whose data was viewed and provided them with information regarding the date(s) and time(s) of access and what portion(s) of their data was seen. (*See id.*)

On 27 May 2015, ICANN additionally provided the affected parties with the name(s) of the user(s) whose credentials were used to view their information without their authorization or by individuals that were not officially designated by their organization to access certain data and any explanation(s) and/or certification(s) that the user(s) provided to ICANN regarding the unauthorized access. (*See* https://www.icann.org/news/announcement-2015-05-27-en.)

With respect to Items 4, 9 and 10, these questions seek information that are not only beyond the scope of DIDP requests as noted above, but are also subject to the following DIDP Defined Conditions of Nondisclosure:

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

- Confidential business information and/or internal policies and procedures.

- Information subject to the attorney– client, attorney work product privilege, or any other applicable privilege, or disclosure of which might prejudice any internal, governmental, or legal investigation.

With respect to your requests for the terms and conditions to which D. Krischenowski agreed, all New gTLD Applicant portal users are subject to the TLD Application System Terms of Use, available at http://newgtlds.icann.org/en/applicants/tas/terms, and the TLD Terms and Conditions, available at http://newgtlds.icann.org/en/applicants/agb/terms. All GDD portal users are subject to the attached Authorized User Terms and Conditions that appear when the user logs in to the portal for the first time.

With respect to your request for correspondence with D. Krischenowski and his legal counsel, this request calls for documents that are subject to the following DIDP Defined Conditions of Nondisclosure:

- Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

- Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

- Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

- Information subject to the attorney– client, attorney work product privilege, or any other applicable privilege, or disclosure of which might prejudice any internal, governmental, or legal investigation.

About DIDP

ICANN's DIDP is limited to requests for documentary information already in existence within ICANN that is not publicly available. In addition, the DIDP sets forth Defined Conditions of Nondisclosure. To review a copy of the DIDP, which is contained within the ICANN Accountability & Transparency: Framework and Principles please see http://www.icann.org/en/about/transparency/didp. ICANN makes every effort to be as responsive as possible to the entirety of your Request. As part of its accountability and transparency commitments, ICANN continually strives to provide as much information to the community as is reasonable. We encourage you to sign up for an account at MyICANN.org, through which you can receive daily updates regarding postings to the portions of ICANN's website that are of interest because as we continue to enhance our reporting mechanisms, reports will be posted for public access.

We hope this information is helpful. If you have any further inquiries, please forward them to didp@icann.org.