Talal Abu-Ghazaleh Domains

TAG-Domains

Newsletter

Issue 52 July 2020

IN THIS ISSUE:

AGIP Awarded Certificate of Appreciation by Dubai Customs

DUBAI – Abu-Ghazaleh Intellectual Property (AGIP) has received a certificate of appreciation from Dubai Customs, in recognition of its essential role in safeguarding Intellectual Property Rights (IPRs) as well as in promoting awareness on the significance of IPR protection,

During the last 10 years, AGIP has worked in close cooperation with Dubai Customs to improve the climate for intellectual property protection, and to encourage the Customs Department to adopt best IP practices.

In this regard, Mr. Amjad Al-Husseini, executive director of AGIP UAE office, said: "AGIP is proud to be recognized by Dubai Customs under the guidance of our Chairman HE Dr. Talal Abu-Ghazaleh. AGIP works in close coordination with Arab governments and multilateral organizations on introducing an efficient IP system in the region."

AGIP has been receiving the Managing Intellectual Property (MIP) Award for being the top IP firm in the Middle East for the last 11 years. In addition, it has been awarded the Best IP Advisor in the Middle East during the 1st, 2nd and 3rd editions of the Innovation & IP Forum and Awards.

What Trademark Owners Need to Know to Avoid Reverse Domain Name Hijacking

A cybersecurity company recently attempted reverse domain name hijacking for an exact match domain name of its brand, and in so doing, failed in both its bid to take ownership of the domain and potentially damaged their reputation by using this somewhat nefarious tactic and abusing the Uniform Domain Name Dispute Resolution Policy (UDRP).
What is reverse domain name hijacking?

Reverse domain name hijacking, commonly known as RDNH in domain name dispute cases, occurs when a trademark owner attempts to secure a domain name by falsely making claims of cybersquatting against a domain name owner.

This is unlike domain name hijacking, which is usually associated with cybercrime where the domain name is stolen through unauthorized access to the domain management account, or domain name system (DNS) hijacking where the name servers for a domain are changed through similar unauthorized access.

In other words, RDNH is where a trademark owner uses UDRP proceedings to coerce an individual domain owner into surrendering their rights to a domain name. This tactic is in breach of the rules, which clearly state that the complainant must certify that they are not using the process improperly as a means to harass a domain holder, and that they are acting in good faith with reasonable argument.

“If after considering the submissions, the panel finds that the complaint was brought in bad faith, for example, in an attempt at reverse domain name hijacking, or was brought primarily to harass the domain-name holder, the panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.” [Internet Corporation for Assigned Names and Numbers’ (ICANN) Rules for Uniform Domain Name Dispute Resolution Policy (Rules), Paragraph 15(e)]2

It’s therefore important that companies fully understand the dispute resolution process in detail to avoid being found to have used this tactic. Furthermore, because cybersquatting is on the rise and third-party registrants are continuing to extort money from legitimate businesses and trademark owners, companies need to understand how to avoid a panel issuing a finding of RDNH against them.

Although a finding of RDNH does not carry a financial penalty, it will go on the public record and taint any future complaint. Panels are also usually quite ruthless in their choice of words, and RDNH is newsworthy, which may lead to reputation damage for a complainant found guilty of RDNH. Finally, RDNH is an offence under the Anti-Cybersquatting Consumer Protection Act, so that U.S.-based domain name

owners may sue in a District Federal Court for damages up to $100,000.
What can companies do to avoid attempted RDNH?

Specifically, in the case of a trademark composed of generic words, or when the domain name has no content, there is an increased risk of the respondent calling for a ruling of RDNH. Trademark owners with sufficient grounds, or who do not display bad faith, are able to avert a RDNH ruling against them.

Trademark owners are recommended to:
Make sure the trademark or the rights predate the domain name registration or acquisition by the last registrant (in case a domain name has changed hands). If prior rights cannot be proven, it will be difficult to claim "bad faith," since under the UDRP, this hinges on registration and use.

Document how the trademark was known at the time the disputed domain name was registered; how well it is known now is irrelevant if the domain name is 20 years older.

Substantiate claims. Don't make allegations in one's favor or discredit the respondent without evidence.

Be honest with the panel. If there was an attempt to buy the domain name from the registrant before starting the UDRP, say so. No panel is going to blame a complainant for trying to recover a domain name more quickly or cheaply than a UDRP, however they're not going to be impressed if a complainant says the respondent tried to sell the domain name to them for an unreasonable fee if the complainant initiated the discussion.

Avoid blatant attempts to entrap the respondent or mislead the panel, for instance, only putting forward incomplete material evidence, details of which then come to light when the registrant files their response.

Finally, carefully consider how and who to trust to file disputes. A boilerplate approach without careful consideration of the facts risks leaving the trademark owner open to not just a loss, but perhaps the accusation of below-the-belt tactics.

Source: CircleID

Verisign Wins US Patent for Blockchain Powered Domain Names

Verisign, a publicly traded company providing domain name registry services, has been granted a blockchain-based patent. Verisign, a major domain name registry that controls the '.com' and '.net' domains, has acquired a patent that applies blockchain tech to domain names.

The United States Patent and Trademark Office (USPTO) granted patent number 10,721,060 to Verisign on July 21. Addresses instead of numbers Titled Domain name blockchain user addresses, the new patent outlines some major benefits and technical advantages associated with registrants utilizing their domain name system (DNS) domain names in a blockchain network.

It can provide the ability to use domain names purchased in the traditional DNS environment in a blockchain environment. Verisign explained that by applying this technology, the registry enables users to turn traditional domains into a "blockchain user address" and interact with other participants on the network.

The technology allows users to use domains as "their blockchain presence,":
"If a registrant owns example.com, they may wish to be able to use it as their blockchain user address. This enables a human friendly way to interact with other blockchain participants by using domain names as addresses instead of numbers [...] it permits blockchain participants to utilize their web presence, e.g., example.com, as their blockchain presence."

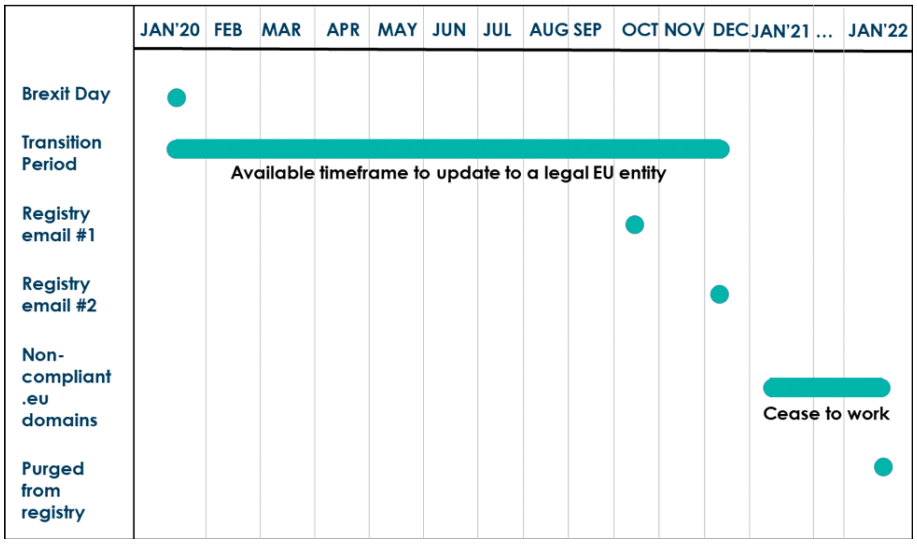
More tools for secure two-factor ID

The patented techniques include management of public and private keys through a DNS registry on the blockchain network as well as operating requests for the so-called "proof of registrar" records. The system enables a blockchain network to receive and store the data about the domain name and its connection with an existing blockchain user address for the registrant.

It can also enable secure two-factor identification by "consulting the blockchain for a given blockchain network." This will unlock additional tools to verify user identity:"For example, if a given address on a blockchain has an attached phone number or email address, those could be consulted on chain as a source to send a message to confirm proof of address ownership." The domain name industry is not new to the crypto and blockchain technology to date. Companies like Unstoppable Domains and MyEtherWallet have been collaborating to enable the crypto community to buy '.crypto' domains that provide decentralized domains. In March 2020, popular browser Opera became the first major browser to integrate the '.crypto' domain extension.

Source: Verisign

How Brexit Raises Risks for Non-Compliant .EU Domain Names



On June 3, 2020, EURid, the registry for .EU domains, published its timeline and action plan to withdraw and delete .EU domains registered to entities and individuals located in the U.K.

Background and Brexit

Following the .EU regulations that were published on March 29, 2019, registrations of .EU domain names may be held by EU citizens, citizens of Iceland, Liechtenstein, and Norway, independent of their place of residence — as well as organizations that are established in the EU. Due to these regulations and subsequently Brexit Day, the day the U.K. formally left the EU, organizations that registered their .EU domains with their U.K. establishments will become non-compliant after the end of the transition period, which is from now until December 31, 2020.

Timeline and action plan

Check that your .EU domain names are registered with entities established in the EU. If any of them are not, modify the registration information in these .EU domain names to those of a legally established entity from one of the eligible EU member states, or be sure to register .UK domain names as alternatives. You must complete any changes by December 31, 2020 because you will not be able to modify any aspect of your .EU domain registrations after January 1, 2021.

What are the risks?

Unless you are not planning on renewing certain .EU domain names after January 1, 2021, there are three immediate risks that you must take note of with regards to this notification:

1. Disruption to VPN, VoIP, website, services, dependencies, servers, networks, or email

If any of the .EU domain names in your portfolio are being used for your organization, the domain names should be updated to full compliance so they continue to work and outlast Brexit's transition period.

Use includes:

Virtual private network (VPN) network
Voice over IP (VoIP) services
A content website
As part of the server infrastructure or network of servers within your organization
A dependent service, like email, web traffic, or any other way you may not be privy to

2. Loss of control and ownership
Non-compliant .EU domains will cease to work after January 1, 2021 and you will lose control of these domains. At that point, you will not be able to modify the domain registration information to make them work. The registry will round them up and make them available for general registration after January 1, 2022, and you will only be able to make attempts at registering them if you fulfill the .EU registration criteria.

3. Hijacked activity trail from abandoned domain names
The core message is reiterate in this article that an abandoned domain name could hurt you. An abandoned corporate domain name often carries a footprint of activity that can be leveraged as an attack vector by cyber criminals. If any of your .EU domain names were receiving email before, they could continue receiving email correspondence from unsuspecting entities that don't know you abandoned the domains. A re-registered domain name gives the new registrant access not only to emails — but also the ability to reset passwords to accounts, like management or financial portals, databases, and social media — giving criminals the opportunity to compromise your business through phishing attacks, data leaks, social engineering, and more.

In addition, if any of your .EU domain names get a certain level of web traffic, you should continue renewing them. KrebsOnSecurity further wrote that such domain names, if not renewed, could pose as a huge security risk to the organization. Reason being, the domain names could then be scooped up by crooks who could use them to set up fake eCommerce sites that steal credit card details from unwary shoppers. These sites capitalize on the visitor traffic that goes towards these sites even after the domain names expire.

Reducing these risks is the rationale behind why EURid will only purge non-compliant .EU domain names after withdrawing them from the active zone for a full year. Although one year may be a long enough period for significant levels of visitor traffic to die down, the other risks are not completely diminished.Resourceful bad actors could still potentially register and restore expired domain names, and leverage them in the aforementioned ways.

What you can do right now
Review your .EU domain portfolio for non-compliance issues that will arise after the end of the Brexit transition period and modify their registration information where possible, and use tools that can help narrow down your vital domains.

Source: CircleID

Please feel free to contact us at:
info@tag-domains.com
Tel.: +962 6 5100 900 ext. 2743
Fax: +962 6 5100 901

HIGHEST SPECS

LOWEST PRICES

TAGTech.Global

Designed and Produced by TAGTech.GLOBAL

TAGTECH @ Best Specs & Prices

Supported by TAG-Foundation

TAG-DC *The DIGITAL Citizen Tablet*

JD 145*

- Octa Core 1.6 GHz CPU
- 10.1" Screen 1200 x 1920
- 4 GB RAM, 64 GB Storage
- Android 9.0 (Pie)
- 5 MP Front Camera and 13 MP Rear Camera.
- Dual SIM Cards, GPS & Bluetooth.
- Wi-Fi: IEEE 802.11 a/b/g/n/ac
- 2G/3G/4G Connectivity.
- Battery Capacity: 6000 mAh.

Free

- Leather Cover with USB Keyboard.
- HQ Bluetooth Earphones and Screen Protector.
- 1 Year Warranty

TAGITOP®-MULTI

JD 453*

- Intel Core i7 6500U
- 8 GB DDR3 RAM
- Intel® HD Graphics Card
- Additional NVIDIA GT940 MX 2GB Graphics Card
- Storage: 1 TB SATA HDD | 128 GB Slot SSD
- Wi-Fi, Bluetooth, HDMI (4K) Output, 2 IN 1 SD/MMC.
- 15.6 Inch Full HD Screen
- 4 USB Ports: 2 USB3.0 , 2 USB2.0
- Chocolate Backlit Arabic\English Keyboard
- Built in Camera

Free

- Carrying Case.
- 1 Year Warranty

TAGITOP®-PLUS

JD 493*

- Intel Core i7 CPU 8550U
- 8 GB DDR4 RAM.
- Intel® HD Graphics Card.
- Storage: 1 TB SATA HDD | 128 GB Slot SSD.
- Wi-Fi, Bluetooth, HDMI (4K) Output, 2 IN 1 SD/MMC.
- 15.6 Inch Full HD Screen
- 4 USB Ports: 2 USB3.0 , 2 USB2.0
- Chocolate Backlit Arabic\English Keyboard
- Built in Camera

Free

- Carrying Case.
- 1 Year Warranty

* VAT Included

Showrooms Open: 9:30 am to 6:30 pm (Saturday to Thursday)

TAG.Global Building 46 Abdel Rahim Al-Waked Street, Shmeisani, Amman, Jordan
TAGUCI Building104 Mecca Street, Um-Uthaina, Amman, Jordan

Tel:+962 65100 909 | Fax: +962 6 5100 901 | Email: info@tagtech.global

TO ORDER ONLINE, PLEASE VISIT: TAGTECH.Global