NATIONAL SHERIFFS' ASSOCIATION

JONATHAN F. THOMPSON
Executive Director and CEO

VIA ELECTRONIC DELIVERY

June 11, 2020

The Honorable Frank Pallone (NJ-06)
Chair
House Committee on Energy and Commerce
Rayburn Office Building, 2125
Washington, DC 20515

The Honorable Greg Walden (OR-02)
Ranking Member
House Committee on Energy and Commerce
Rayburn Office Building, 2125
Washington, DC 20515

Dear Chairman Pallone and Ranking Member Walden:

On behalf of the National Sheriffs' Association, I write to thank you for your dedication in responding to the global COVID-19 pandemic and to ask for **your immediate action to reinstate a vital law enforcement tool that can be taken to protect American consumers from counterfeit medications, frauds, scams, and other dangerous products claiming to be related to the pandemic.**

While the value of WHOIS data is widely known throughout the law enforcement community, its day-to-day use is less known elsewhere. We are gravely concerned about the overly broad interpretation and damaging implementation of the European Union's General Data Protection Regulation that has effectively blocked access to this critical data set and the time has come for Congress to engage on this important issue.

As you may know, WHOIS data is the publicly available information on *who* has registered a particular internet domain name. In layman's terms, WHOIS records are akin to land title or property tax records: a record of who owns the internet property of domain names available in .com, .net, and other generic top-level domain (gTLD) spaces. Each WHOIS record contains basic contact information for the domain name registrant: name, address, phone number and email address, and certain other technical attributes. Since the dawn of the internet as we know it, gTLD registrars and registries – those companies who sell domain names – have collected contact information from all registrants at the time of registration.

Law enforcement and third-parties have historically had access to this information and used it significantly in investigations and prosecutions against online crimes, including selling illegal online pharmaceuticals, human, child, and animal trafficking, intellectual property theft as well as cyber-attacks and misinformation campaigns. It is often said that "sunlight is the greatest disinfectant." To that end, WHOIS information provides transparency to who is behind a particular website or domain name.

Congress must act to require transparency to stop internet fraud at scale. As Rep. Bob Latta (R-OH) called for in a February 2020 House Resolution[1], Congress should require registrars to validate domain name registration information and make registration data accessible.[2] **The US DOJ, FTC, FDA, Department of Commerce, Europol, cybersecurity experts, public health leaders, and others agree that access to domain registration information is the essential for "tracking down cybercrooks and/or for disrupting their operations."[3]**

The pandemic has led to an explosion of cybercrime, preying upon a population desperate for safety and reassurance. These criminal activities require domain names, which are being used to run illegal drug, phishing, spam, and malware campaigns, and scam sites. During March 2020, at least 100,000 new domain names were registered containing terms like "covid," "corona," and "virus",[4] plus more domains registered to sell items such as medical masks. Beyond this, other domains were used to spam out advertisements for COVID-themed scams. New domain names fitting these criteria are being registered at the rate of around 1,000 per day.[5] Websites, social media, and online marketplaces will remain constant sources of healthcare scams unless Congress takes concrete action to address structural issues that have enabled online frauds to proliferate.

WHOIS data is critical to law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, intellectual property rightsholders, journalists, academics, election security officials and others. These stakeholders all rely on WHOIS to help them determine who is operating a criminal website, sending malicious (spam, phishing) emails, conducting cyber-attacks, influencing elections, propagating fake news or committing fraud under the guise of a known brand. In these instances, WHOIS data is used to identify and collect lists of domain names that investigators associate with a given criminal or cyber-attack and to identify the likely perpetrators of these attacks. In criminal investigations, for example, listing domains and making connections using contact information is imperative to understanding and interdicting criminal, terrorist, or hostile nation state activity to its fullest extent.

The COVID-19 pandemic makes your work against healthcare and financial fraud more important now than ever. Please do consider us a resource and ally in this fight.

Sincerely,

Jonathan F. Thompson
Executive Director and CEO

[1] https://latta.house.gov/uploadedfiles/latta_whois_house_resolution.pdf
[2] https://latta.house.gov/news/documentsingle.aspx?DocumentID=402281
[3] See https://secureandtransparent.org/policy-and-advocacy/
[4] Don't Panic: COVID-19 Cyber Threats." Palo Alto Networks Unit 42 blog, 24 March 2020, at: https://unit42.paloaltonetworks.com/covid19-cyber-threats/
[5] "Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN." Interisle Consulting Group, LLC, 31 March 2020, page 18, at: http://bit.ly/DataCrossroads