February 19th, 2021

Written Submission in Advance of the 2021 Budget

The Alliance for Safe Online Pharmacies Canada (ASOP Canada) is pleased to provide a submission to the 2021 Pre-Budget consultation. As outlined below, COVID-19 has increased the public health threat of illegal online sellers of medical products, which requires immediate funding and resources by the Government of Canada to combat this threat and support enforcement ensuring a more resilient Canada once COVID-19 is under control.

ASOP Canada is a project of ASOP Global, a global non-profit organization dedicated to keeping the public safe from illegal online sellers of prescription medicines and protecting the integrity of our legitimate pharmaceutical supply chain. We have a diverse membership that includes pharmacists, pharmacies, distributors and our observers include the National Association of Pharmacy Regulatory Authorities (NAPRA), Canadian Patient Safety Institute (CPSI), GS1 Canada, among others.

Recently, ASOP Canada sponsored a survey, conducted by Abacus Research to test consumer attitudes toward purchasing online, and if those attitudes have been shaped by the COVID-19 outbreak. The survey revealed an upward trend of Canadians purchasing medications online compared to a survey we conducted a couple of years ago. In addition, the survey found that a majority of Canadians are open to purchasing medicines or medical products online. A concerning statistic found that 4 in 10 Canadians are willing to take risks and access sites that have not been verified by an appropriate licensing body, if it meant accessing medications otherwise not available or available at a lower cost. With the normalization of both digital health care and online purchasing of medical products during COVID-19, Canadians need to be assured that their health is being protected when accessing health care and products online.

At the same time, over the past few months, we have seen an increase in misinformation over the internet, and enterprising individuals and organizations seeking to take advantage of Canadians feeling vulnerable and situated at home by making false or misleading claims about products to address COVID-19. Many of these products were found through online sources. This issue is not limited to products for COVID-19; controlled substances including opioids, other prescription medications and medicinal cannabis are sold through unlicensed sites, causing harm through inappropriate use or selling counterfeit drugs.

In order to avoid further risks to Canadians, we believe that collaboration across multiple stakeholders is needed, to support and provide the resources required for activities such as public awareness, education, research and enforcement.

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 phishing, spam, and malware campaigns, and scam sites.[1]

- During March 2020, at least **100,000 new domain names** were registered containing terms like "covid," "corona," and "virus,"[2] plus more domains registered to sell items such as medical masks.[3] Beyond this, other domains were used to spam out advertisements for COVID-themed scams.

[1] "The Internet is drowning in COVID-19-related malware and phishing scams." Ars Technica, 16 March 2020, at: https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malwareand-phishing-scams, and "Coronavirus Used in Malicious Campaigns." Trend Micro, 20 March 2020, at: https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/coronavirus-used-inspam-malware-file-names-and- malicious-domains.

[2] "Don't Panic: COVID-19 Cyber Threats." Palo Alto Networks Unit 42 blog,24 March 2020, at: https://unit42.paloaltonetworks.com/covid19-cyber-threats/ .

[3] "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.

- As of March 2020, the number of confirmed malicious COVID-related domains is in the thousands.
- New domain names fitting these criteria are being registered at the rate of around **1,000 per day**.[4]
  - Nearly 6,500 of those domains have the ability to send and receive email - which is a strong indication that they could be used in phishing, fraud or business email compromise attacks.
  - 122 of the names also contain the string "vaccine" and over 400 contain the string "test" with well over 20% of both sets of names also ready to send and receive email.

With the significant increase of medical product cybercrime during COVID-19, the likelihood of Canadians continuing to use these online sources for medial products significantly increases along with the threat to public health that drugs to treat disease and illness are purchased from these illegal sources.

In order to combat the increase in cybercrime that Canada is experiencing today, and protect Canadians after COVID-19 is handled, domain name registries and registrars (R/R) must act to stop online COVID-19 scams, and sales of illicit opioids and of counterfeit or unapproved prescription drugs.

- R/Rs have the power to stop massive amounts of public health harms and fraud online.
- R/Rs should immediately, upon notice from a credible party, lock and suspend any domain name that is used to facilitate the COVID-19 scams and the illegal online sales of medicines and illicit drugs.
- Some Canadian-based R/R will shut down (i.e. lock and suspend) rogue websites based on information from trusted third-party notifiers like Canadian Anti-Fraud Centre, RCMP, Health Canada, and others. But many others do not and often serve as safe-havens for illicit activity.
- Especially during a Public Health Emergency, we need all actors – including R/Rs – to do whatever they can to stop online COVID-19 frauds and the illegal sale of healthcare products online.

Experience has shown that registries and registrars often will not act to prevent public health harm online without a specific court order. This has been true even when:

- The domain names themselves explicitly imply illegal activity (e.g. www.covidcures.com).
- The R/R has been notified by a trusted third-party that certain domain names on their platforms are being used in violation of the R/R's own contracts (terms of agreements).
- The R/R has knowledge that a domain name is unequivocally being used to sell opioids, offer COVID-19 "cures," or otherwise endanger public health and safety.

R/Rs are profiting from licensing domain names that create and/or exacerbate existing public health harms. This puts lives at risk, especially in a Public Health Emergency when millions of Canadians are sheltering in place and rely on the internet for access to healthcare information, products, and services.

Historically, public and private cyber investigators and first-responders could "triage" attacks by obtaining information about thousands of domain names using a service called WHOIS in near real-time.

- These parties are responsible for the majority of the more than two billion WHOIS queries every day, most of those in automated fashion, to track and measure the proper functioning of domain names, and to judge the risks they pose.
- But over the last two years, access to WHOIS data has been drastically curtailed as a result of ICANN policies, the EU data privacy laws, and to the elective practices of registrars and registries.

[4] Id.

COVID-themed attacks are easier to conduct and harder to mitigate because domain industry policies and business interests interfere with the acquisition of information that's essential to investigation, identification, mitigation, and apprehension of the criminal actors.

- In a correspondence to registrars GoDaddy, NameCheap, Register.com and others, the NYC Office of the Attorney General states that, "the current environment demands the highest vigilance" and has asked the registrars for proactive steps to prevent, find, and suspend these malicious domains.
- The U.S. Department of Justice notified registrar NameCheap that "Communications facilitated by your entity and made by your direct customers or business partners have been linked to [such] criminal activity", referring to fraudulent schemes targeting U.S. citizens exploiting the current COVID-19 pandemic.

Immediate action is required to protect Canadian citizens from ongoing harm and to maintain the trust and integrity of the internet during a time where it is relied upon most:

- Registrars must lock and suspend when COVID-themed domain names are suspicious or when first responders provide evidence that they are harmful.
- To maintain internet security and transparency, legislation is needed to require registries and registrars to provide open access to WHOIS records that are accurate, non- anonymous and accessible at scale.

While the Government of Canada looks towards creating a resilient Canada post-COVID-19, there are significant issues that need the support, resources, and funding to combat illicit industries that have taken advantage of the pandemic. ASOP Canada thanks the Government of Canada and Finance Committee for the opportunity to submit in the 2021 Pre Budget Consultation and look forward to working with the Government in finding ways to protect Canadians and curtail future threats to public health.