Illicit Trade at the time of the COVID-19 Crisis
OECD TF-CIT Webinar
April 23, 2020 | 2:00pm CET

ASOP EU Statement

EXECUTIVE SUMMARY

The Organisation for Economic Co-operation and Development (OECD) held a webinar with its members and stakeholders to determine how the current COVID-19 crisis is impacting on illicit trade. Its specific objectives were to understand if there were changes in illicit trade flows and how these may evolve, and so determine how governments might respond. In addition, solutions to the criminal activity were also tabled.

The rising tide of illicit trade via the Internet formed an important part of the debate. The Alliance for Safe Online Pharmacies Global (ASOP Global) and the Alliance for Safe Online Pharmacy in the EU (ASOP EU) has an established track record in all things to do with combatting illicit online trade of falsified, substandard or counterfeit medicines for many years now. The Intervention given by ASOP EU outlined clearly two specific and achievable solutions that, if implemented would drastically improve the governance of trade transacted over the Internet and thus drastically reduce criminal activity.

Solution Number 1 – Addressing the Domain Name Registration System and WHOIS Access. 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. So we need to lift the veil of secrecy that companies are hiding behind.

Solution number 2 – Access to and the acquisition of domain names. Specifically, these internet intermediaries are registries and the registrars who must now completely and comprehensively uphold DOMAIN INDUSTRY ACCOUNTABILITY. Efforts should be proactive and responsive to pervasive threats to user health and safety, not just for COVID-19 related frauds but the variety of other threats that are present online. This means that:

- 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 U.S.-based R/R will shut down (i.e. lock and suspend) rogue websites based on information from trusted third-party notifiers like LegitScript, U.S. FDA 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.

ASOP EU'S SUGGESTED INTERVENTION

I would like to begin by thanking the OECD for setting up this important meeting. I believe that together we can achieve something very significant in the coming months as we shape our international response to the current circumstances. Paradoxically, the current COVID-19 pandemic may have a silver lining, in that it will enable us to get practical, feasible, understandable, actionable initiatives that will greatly enhance public safety throughout the world. We recognize and appreciate the clear public health and consumer safety implications of a swift and comprehensive response. ASOP EU will propose two actionable solutions that will we believe will make a huge difference but before I do, let me explain the context from which these solutions are derived.

The Alliance for Safe Online Pharmacies Global and the Alliance for Safe Online Pharmacy in the EU – ASOP Global and ASOP EU, respectively – have been deeply involved in all things to do with combatting illicit trade of falsified, substandard or counterfeit medicines for many years now. Led by ASOP Global and the National Consumers League, 43 stakeholder organizations collectively penned a letter to United States Vice President Mike Pence and other senior administration officials that recommends measures to address a variety of harms related to COVID-19 fraud and misinformation, including the structural Internet Policy problems that enables these scams..

The fact that during March 2020, at least 100,000 new domain names were registered containing terms "covid," "corona," and "virus", and domains registered to sell items such as medical masks, makes this letter all the timelier and more impactful. We also understand that additional research is underway to better capture and understand the implications of what is available to consumers online and how it may ultimately impact the international response.

And now some observations:

1. **Observation One**. We do have ICANN. And it drives a lot of what goes on in the Internet. However, it has conflicting priorities and objectives which slow initiatives down. A classic example of this is its interpretation of GDPR which has essentially blocked transparency of the WHOIS database on the Internet. However, we would advocate a centralization of decisions by ICANN that are pro-active and sets out to properly cure the ills on the Internet.
2. **Observation two.** International trade, year after year is transacted more and more via the Internet. E-Commerce is massive and growing with both supply and demand increasing in lockstep. The Internet makes the trade largely borderless as small parcels arrive in to our countries largely unseen and unheeded. Yet governments and institutions at present have to rely on systems that in some cases is like looking for a needle in a haystack.

In response, it is clear that we need a global body and collective policy that can be used both regionally and nationally. By and large, the Internet operates outside of government reach and can serve as safe harbours for illegal activity. After all the contracts within the Internet ecosystems are with private companies who can adopt whatever policies they wish to institute. Of course, this does not apply to all Internet actors but it does allow bad actors to roam the web freely and largely undiscoverable and therefore unaccountable. So we need a collective, co-ordinated and focused response. **And that begins at the source – those who control domain names.**

ASOP Global's proposal, which has been developed and refined over a number of years, is based on a deep understanding of what is needed to rectify the situation from criminal online activities relating to illicit trade. The two proposals I am going to outline now are inter-connected and both gain synergistic strength together.

Solution number 1 - to focus on the domain name registration system – that is the beginning of everything. Your URL, your email and other internet thoroughfares are derived from the domain name system.

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.

COVID-themed attacks are easier to conduct and harder to mitigate because domain industry policies and business have essentially shut down a major law enforcement interrogative portal on who is doing business on the Internet.

WHOIS portal information is critical in accessing the requisite information around website operations. How can it be possibly right when we are identifying hundreds of thousands of fraudulent COVID-19 websites and related scammers? Current practices are such that most registrars require a ponderous court injunction system before they will take action. How can it be right that businesses are allowed to trade freely and illegally without any transparency on how they operate?

In turn, we need to lift the veil of secrecy that companies are hiding behind. And it is encouraging to note the following from ICANN, and I quote:

> *Combating abuse requires predictable and reliable access to domain name registration data for those with a legitimate interest. ICANN org continues to try to gain clarity under the European Union's General Data Protection Regulation with regard to whether a Unified Access Model for gTLD domain name registration data is possible under EU law. Access to this registration data is critical for law enforcement and security practitioners to protect Internet users from the criminals leveraging the COVID-19 pandemic, or any other threats that emerge, for fraudulent and criminal activity.*

So that's solution one – make the WHOIS data base viewable by all and maintain an internet that has security and transparency at its core. I'd like to reiterate the critical nature of these internet resources. And so, legislation in each and every jurisdiction is needed to require registries and registrars to provide open access to WHOIS records that are accurate, non-anonymous and accessible at scale.

Solution number two is all to do with access to and the acquisition of domain names. Specifically, these internet intermediaries are registries and the registrars who must now completely and comprehensively uphold DOMAIN INDUSTRY ACCOUNTABILITY. Efforts should be proactive and responsive to pervasive threats to user health and safety, not just for COVID-19 related frauds but the variety of other threats that are present online. This means that:

- 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 U.S.-based R/R will shut down (i.e. lock and suspend) rogue websites based on information from trusted third-party notifiers like LegitScript, U.S. FDA 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.

Why can't countries pass laws that simply say to registries if you want to operate you have to do so legally which means that when you on board a business entity you require absolute proof of identity and that when a registrar onboards a client the same principle applies. A good example of such a good practice can be seen in Denmark where they have a law which covers this and they have seen a massive reduction in suspicious and potentially criminal activity.

So to conclude ASOP EU recommends two solutions: Unveil the WHOIS data base and equally importantly, control access to domain names by policy and legislative change to ensure registries and registrars are fully accountable.

And all this can be augmented by an authoritative and empowered global over-arching centralised decision-making body.

M P Isles
23 April 2020