Countering Covid-19 Criminality: Battling Pharmaceutical Cybercrime

Grant Courtney

Perhaps the most eagerly anticipated therapeutic innovation in the history of time, the first effective Covid-19 vaccine is now rolling off the production line and out to the world.

Producing and successfully distributing an effective vaccine has signaled a significant step towards addressing a global pandemic that has crashed economies, curbed freedoms, claimed close to 1.5 million lives worldwide and sickened more than 63 million. Projecting into the not-too-distant future, the fully vaccinated will be able to enjoy greater freedoms; to interact, to travel, to work and to return to some sense of normality. That the ticket to these freedoms is potentially contained in a small glass vial, makes these vials at high risk of falsification and counterfeiting by criminals seeking profit from the misfortune and fear of others.

I have written before about the importance of using established traceability standards to secure the legitimate vaccine supply chain. However, to truly and effectively protect the legitimate supply chain, we must not overlook the illegitimate one. One of the most significant contributing channels in the illegitimate pharmaceutical supply chain is cybercrime, more specifically the sale of falsified medicines online. Cyber-criminal organisations haven't lost time in exploiting the Covid-19 pandemic. If anything, they've been quick to shift towards a new area of growth and profitability, one that is driven by the fear and uncertainty that accompanies the pandemic-related morbidity and mortality. Fortunately, governments, pharmaceutical companies and trade associations have spent decades keeping pace with the ever-evolving tactics of cyber criminals.

A recent report from the National Association of Boards of Pharmacy (NABP) identified dozens of sites where falsified or bogus Covid-19 treatments are offered. Sometimes these sites were already operating and only added coronavirus-related images to profit from the pandemic. Other sites have purchased domain names including Covid-19 key words, such as 'covid', 'corona' and 'virus', drawing visits from unsuspecting or desperate users but also raising red flags.

A two-pronged offensive

As the techniques used by the sellers of illicit medicines are becoming more and more sophisticated, so too is the fight against them. There's a dual strategic attack on cybercrime at play. Firstly, an effort to educate the public about legitimate internet pharmaceutical commerce sites. This is accompanied by mechanisms to police the most popular e-commerce platforms, such as eBay and Amazon, and secure the buy in of internet infrastructure providers in an attempt to stamp out dubious sellers.

Grant Courtney is a leading healthcare industry consultant and industry-recognised expert adviser on digital brand protection and product traceability. He examines the challenges the world faces at the advent of a Covid-19 vaccine, with the surge in illicit Covid-19 medical products and looks to recent developments in the fight against rogue online pharmacies.

e: grant.courtney@be4ward.com

t: +44 (0)800 098 8795 ext. 1974

Be4ward®

Policing the sellers

Since the start of the pandemic, Amazon has suspended tens of thousands of sellers of illicit medicines, in collaboration with the US and European authorities. Regulatory bodies have also contributed to this online offensive. In April, the UK's Medicines and Healthcare products Regulatory Agency (MHRA) suspended 9 domain names and social media accounts selling fake or unauthorised Covid-19 products. Since March 2020, the U.S. Food and Drug Administration (FDA) has issued more than 140 warning letters to individuals and companies for unapproved or misbranded products related to the pandemic. The agency's *Operation Quack Hack* alone netted hundreds of online marketplaces alleging availability of Covid-19 preventatives, treatments and cures.

Major players in the fight against pharmaceutical cybercrime are two non-profit patient safety organisations: the European Alliance for Access to Safe Medicines (EAASM), and the Alliance for Safe Online Pharmacy in the EU (ASOP EU). These organisations have spent the last decade raising public awareness of falsified medicines, with campaigns like *Counterfeiting the Counterfeiter* and *Facts about buying fake medicines*. This last campaign ran in five countries (France, Germany, Italy, Spain and the UK) and with over 35,000 first page search results per day, it demonstrated the public interest in buying medicines online.

ASOP EU is currently trying to get traction from search engines, online marketplaces and social media platforms to integrate artificial intelligence into their platforms, to identify rogue websites and online sellers and automatically demote them in results. Placement in later pages will effectively remove them from immediate access by consumers. This has proved successful in the field of illegal streaming of videos and could likely be repurposed for pharmaceutical sales online but would require a willingness by the search, social and online marketplace companies to focus on solving the problem.

A crucial element in policing this form of cybercrime is the required buy-in and monitoring by internet infrastructure providers, such as domain name registries and registrars. Domain name registrars sell domain names to registrants, the end-user or operator of a website. Domain name registries operate the top-level domain itself, like *dot com* and *dot pharmacy* and contract with registrars to sell domain names. ASOP EU has launched an effort to involve domain name registries and registrars in the fight to protect patient safety online. ASOP EU believes that the Digital Services Act (DSA), the EU plan to regulate digital services, should mandate that registries and registrars maintain a transparent registrant database, called the WHOIS record, for domains used for commercial purposes, with proof of identity.

For more than 25 years, WHOIS has required domain name registrants to provide correct and verifiable contact information, including name, address, phone number and email address upon registration. Combined with certain other attributes of a domain name's registration, this is collectively called WHOIS data. Authorities such as the US FDA, the UK MHRA, and trusted third-party notifiers such as LegitScript, NABP and others could use the WHOIS data to inform registries and registrars of domain names used to facilitate Covid-19 scams, illegal online sales of medicines, and illicit drugs. EU and US authorities and cybercrime experts have also weighed in on the importance of WHOIS data transparency.

Requiring domain name registration data transparency would strike a blow at the core of online falsified medical product networks by limiting their ability to operate anonymously. Most belong to organised criminal networks that have already been targeted by authorities such as the FDA and European law enforcement authorities. These rogue networks create website templates and run back-end services such as payment processing and product shipping. The website templates are then run by 'affiliate marketers' who operate them, drive traffic to the illicit websites and take a small cut of the profits. These multiple links create multiple opportunities for law enforcement to identify rogue actors within a database. The weak links in an online illicit pharmacy operation would lead to its demise.

EAASM and ASOP EU have been at the forefront of efforts to translate internet policing programmes into legislation. The scale of the problem is immense, and a huge part of the problem is the very existence of the customer base. Afterall, if the public was not there to create the demand, the supply would not be needed.

Educating the world – knowledge is power

ASOP EU and EAASM recently conducted a joint survey, which found that between 35% and 58% of citizens of the five largest EU members have bought medicines online. This tracks along with ASOP Global's recent consumer survey from July 2020 which found 35% of Americans purchasing prescription drugs online, up from 33% in 2017. Confidentiality, convenience, speed and savings were the most common reasons invoked.

Most respondents, from 36% and 85% depending on the country, weren't aware of the need for online pharmacies to display the common EU Falsified Medicines Directive logo.

Encouragingly, more than 90% said they would change their online behaviour and seek out an authentic online pharmacy or go to their bricks and mortar local pharmacy after learning about the magnitude of the problem and the existence of websites selling illicit medicines. The study essentially showed a woeful lack of knowledge of these websites and few were aware of the Common Logo, which each legitimate EU online pharmacy must display. This problem exists with healthcare providers too, in that they are unequipped to effectively counsel patients on illegal online drug sellers or counterfeit medications. More than half could not distinguish a legitimate online pharmacy website from an illegitimate site.

Raising awareness of the use of the internet domain dot pharmacy, currently well established in North America for legitimate online pharmacies, is a further initiative to counter pharmaceutical cybercrime. The Pharmacy Verified Websites Program is operated by the National Association of Boards of Pharmacy and aims to provide a safe and legitimate source of prescription drugs and related content online. Additionally, EUrid which operates the .EU country code top level domain name has more than two million websites and has a memorandum of understanding with ASOP EU to examine suspicious websites monthly.

ASOP EU has proposed the use of the *dot pharmacy* top-level domain across all the Member States so in Germany it would be *dot apotheek*, in Spain *dot pharmacie*, in Italy *dot farmacia* and so on. Some registries have more than stepped up to the mark to 'clean' their platform of websites selling illicit medicine. As a broader intervention, the use of country-specific *dot pharmacy* domains could serve to provide individuals with a tool to help legitimise the practice and provide consumers with a method to verify safety online.

These examples illustrate just a handful of the many organisations devoted to making the world of online pharmaceuticals a safer place. Covid-19 vaccine related cybercrime is by no means a new supply chain protection issue, yet it is evolving and although we can learn from past lessons it is important to keep pace with these developing markets.

Raising awareness, education and effectively removing the customer base from this illicit trade is of significant benefit. This will be all the more effective alongside the support of and active monitoring by brand owners, manufacturers and the big e-commerce platforms and the introduction of more robust legislation, trusted site signals and enforcement. As with many issues, the Covid-19 pandemic has pulled the practice of rogue online pharmacies into the spotlight, further serving to help the global education effort. Yet it is only through the engagement of all the key stakeholders that the battle will be won.

ASOP EU Facts and Tips

The facts

- Over 35,000 websites sell illegal medicines
- 95-96% of websites selling medicines are operating illegally
- Fake medicines may have too much, too little or no active ingredients
- Fake medicines may contain poisons such as paint thinners and other deadly ingredients
- Fake medicines are often made in unsanitary and non-sterile environments

Top tips

Don't buy from an online pharmacy that:

- Does not have a licensed pharmacist, or physical address and a telephone number that works
- Offers bulk discounts or 'amazing' claims and results
- Does not require a valid prescription for prescription medicines. This tells you straight away it is operating illegally
- In Europe does not display the common logo

New:
EU common logo
Click to verify if this website is operating legally

The 'EU Common Logo', introduced by a European Directive, will include your county's national flag and link you to the website of the national competent authority, listing all legally operating online pharmacies.

http://www.ema.europa.eu/ema/index.jsp?curl=/pages/regulation/general/general_content_000630.jsp

Alliance for Safe Online Pharmacy
https://buysaferx.pharmacy/eu/

European Alliance for Access to Safe Medicines
https://eaasm.eu/en-gb/

Medicines and Healthcare products Regulatory Agency
https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency

National Association of Boards of Pharmacy
https://nabp.pharmacy/

Counterfeiting the Counterfeiter report:
https://eaasm.eu/wp-content/uploads/CtCreport2012.pdf

Facts about Fake Medicines report:
https://onlinepatientsafety.org/