Memo: COVID-19 Cybercrimes
Submitted to the Standing Committee on Health (HESA)
May 17, 2021

The Alliance for Safe Online Pharmacies Canada (ASOP Canada) is pleased to provide an updated briefing to the Standing Committee on Health, concerning the threat of COVID-19 related cybercrimes to public health and safety in Canada. ASOP Canada submitted an initial statement to the Standing Committee in July 2020.

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.

COVID-19 related cybercrimes include the sale of counterfeit vaccines, other medicines, and PPE; misinformation, including remedies; and counterfeit vaccine certification documents. As demonstrated below, criminal COVID-19-related activities presents a risk to Canadian health and safety, and as such requires action by the Government of Canada.

The illegal online sale of counterfeit medicine is not new. Criminal actors have long used the online market to sell controlled substances, including opioids, other prescription medications and medicinal cannabis through unlicensed sites, causing harm through inappropriate use or selling counterfeit drugs. These same criminal networks have now moved into the space of COVID-19, preying upon the uncertainty and fear of the public to sell one of the most globally sought-after products, COVID-19 vaccines.

Simultaneously, 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 and often lead to websites spreading malware and stealing Canadians personal information.

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.

Cybercrime at a Glance

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]

[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 .

Beyond this, other domains were used to spam out advertisements for COVID-themed scams.

- 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.

Illegal Online Sales – COVID-19 Vaccines

A search engine scan or social media post can open unsuspecting individuals to local and international criminal networks. As vaccine supply chains and availability have become uncertain, criminal actors have taken advantage of this uncertainty and have begun to prey on the public through a medium that has become critical to information, health care, and business – the internet.

On March 31st, 2021, the Canadian Anti-Fraud Centre, a government program supported by the RCMP, Competition Bureau and OPP, issued a public warning to Canadians to avoid purchasing vaccines online or through unauthorized sources. In addition to highlighting the risks associated with purchasing potential counterfeit COVID-19 vaccines from private companies outside Canada's legitimate pharmaceutical supply chain, the CAFC's Jeff Thomson indicated ""People are looking to get the vaccine. They want to return to normal sooner than later. So like other frauds, these frauds are playing on emotion." [5]

The **global spike in cybercrime and marketplace for counterfeit vaccines vary from international sophisticated smuggling networks to local criminals filling used genuine vaccine vials and selling the unknown materials online.** Examples of the latter can be found below:

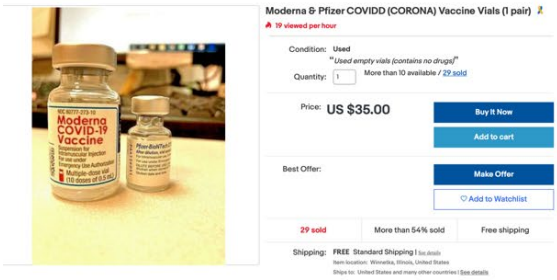

Image provided by Partnership for Safe Medicine

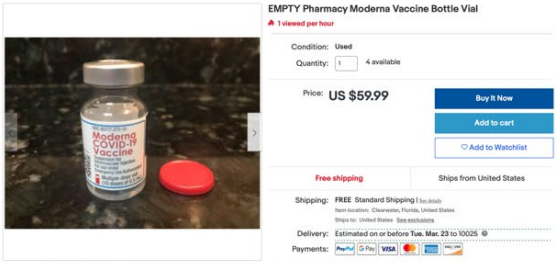

Image provided by Partnership for Safe Medicine

Image provided by Partnership for Safe Medicine

Internationally, INTERPOL has been a leader in both raising awareness and enforcement in COVID-19 related cybercrime. As part of **INTERPOL's Illicit Goods and Global Health (IGGH) Programme**, INTERPOL worked with local authorities in South Africa to stop **2,400 vials of fake COVID vaccines** reportedly manufactured in China and

[4] "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.

[5] Canadian Anti-Fraud Centre warns of COVID-19 vaccine scams https://globalnews.ca/news/7742030/canadian-anti-fraud-centre-warns-vaccine-scams/

smuggled into the country in March 2021.[6] After the takedown, the General Secretary of INTERPOL, Jürgen Stock commented, "I've never seen such a dynamic situation before," adding that "[t]he liquid gold in 2021 is the vaccine, and already we are seeing that they [vaccine supply chains] are targeted more and more."[7] Another seizure took place in China, where police identified a network selling counterfeit COVID-19 vaccines overseas and resulted in the **seizure of more than 3,000 fake vaccines**.[8]

There have also been several examples of online sites being created to sell counterfeit vaccines and spread fraud. **U.S. Homeland Security** has seized more than **$49.1 million in illicit COVID-19 products, with 80,002 COVID-19 related domains analyzed, 30 websites taken down, and 281 criminal arrests**.[9] In December 2020, Homeland Security **seized two websites claiming to be legitimate biotechnology companies developing treatments for the COVID-19 virus**. One of these sites was a fraudulent Moderna website, modernatx.shop. The site offered advance purchase of vaccine at $30/dose, but never delivered any product and instead was used to collect the personal information of individuals visiting the sites to use the information for criminal purposes, including fraud, phishing attacks, and/or deployment of malware.[10]

Global Activities

The increase in COVID-19 related cybercrimes has led to several **international and national enforcement and regulatory organizations actively raising awareness and enforcement in this area.**

INTERPOL

On December 2nd, 2020, INTERPOL issued a global alert to law enforcement across its 194 member countries, warning them **to prepare for organized crime networks targeting COVID-19 vaccines**, both physically and online. The Orange Notice outlined potential criminal activity concerning the "falsification, theft and illegal advertising of COVID-19 and flu vaccines, with the pandemic having already triggered unprecedented opportunistic and predatory criminal behaviour."[11] As part of the alert, INTERPOL **highlighted the need for a coordinated effort between health regulators and law enforcement to tackle this threat.** Three months later, INTERPOL took down the two counterfeit vaccine criminal networks described above.

INTERPOL also alerted members of **3,000 websites associated with online pharmacies suspected of selling illicit medicines and medical devices, of that 1,700 contained cyber threats**, especially phishing and spamming malware.[12]

On March 24th, 2021, INTERPOL and the U.S. Homeland Security Investigations (HSI) partnered to warn against the online purchasing of alleged COVID-19 vaccines and treatments. The **warning linked criminal groups to the ongoing threat of online scams and counterfeit vaccines and cautioned that cybercriminals are setting up illicit websites that claimed to be legitimate national and/or world organizations offering pre-orders for vaccines against the COVID-19 virus.[13]**

[6] "Fake COVID vaccine distribution network dismantled after INTERPOL alert", INTERPOL, March 3, 2021, at: https://www.interpol.int/en/News-and-Events/News/2021/Fake-COVID-vaccine-distribution-network-dismantled-after-INTERPOL-alert
[7] Ibid.
[8] Ibid.
[9] "Operation Stolen Promise – One Year Anniversary", United States Homeland Security at: https://www.ice.gov/topics/operation-stolen-promise
[10] "How Counterfeit Covid-19 Vaccines And Vaccination Cards Endanger Us All", Judy Stone, Forbes, March 31, 2021, at: https://www.forbes.com/sites/judystone/2021/03/31/how-counterfeit-covid-19-vaccines-and-vaccination-cards-endanger-us-all/?sh=6e4cb3143649
[11] "INTERPOL warns of organized crime threat to COVID-19 vaccines", INTERPOL, December 2, 2020, at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines
[12] Ibid.
[13] "Online vaccine scams: INTERPOL and Homeland Security Investigations issue public warning", INTERPOL. March 24, 2021, at: https://www.interpol.int/en/News-and-Events/News/2021/Online-vaccine-scams-INTERPOL-and-Homeland-Security-Investigations-issue-public-warning

WORLD HEALTH ORGANIZATION

On March 26th, 2021, the World Health Organization (WHO) issued a **Medical Product Alert after counterfeit vaccines were detected in Mexico in February 2021**. WHO confirmed that the falsified product was supplied and administered to patients outside authorized vaccination programs.[14] WHO warned that the **counterfeit vaccine may still be in circulation in the region of the Americas** and accessible to the public. The WHO suggests that organized criminal networks are target medicine and vaccine trade because "it is relatively safe—profits are high, risk of successful prosecution is low, and there are small penalties."[15]

UNITED STATES

In April 2020, the United States organized a **multi-agency program** to tackle the increasing threat of COVID-19 related fraud and criminal activity. The program, Operation Stolen Promise, involved U.S. Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI), working closely with U.S. Customs and Border Protection. Operation Stolen Promise's initial focus was "combatting the illegal import and sale of counterfeit/substandard products; detect and deter financial fraud scams; and prevent the exploitation of relief and stimulus program."[16] The program was **expanded in 2021 to focus on the countering of the new and evolving public health threat posed by the illicit sale and distribution of counterfeit or unauthorized vaccines and treatments**." [17]

Operation Stolen Promise had a four-pronged approach: Partnership, Investigation, Disruption, and Education. After one year, the Program has resulted in:

Focus 1 – COVID-19 Fraud	Focus 2 – Combatting COVID-19 Vaccine Fraud
• 2,121 COVID-19 related seizures (prohibited COVID-19 test kits, prohibited pharmaceuticals, counterfeit marks) • 281 criminal arrests • $49.1 million (USD) illicit proceeds seized • 80,002 COVID-19 related domains analyzed • $32.9 million Cares Act fraud seizures	• 74 seizures • 38 cases initiated • 8 criminal arrets • 30 websites removed

Source: Operation Stolen Promises, Homeland Security

On March 1st, 2021, the U.S. Food & Drug Administration released a consumer alert warning Americans of the threat of both counterfeit vaccines and fake treatments. The FDA defined **fraudulent COVID-19 products as "dietary supplements and other foods, as well as products claiming to be tests, drugs, medical devices, or vaccines."[18]**

The **FDA worked with retailers to remove misleading products from stores and online and continues to monitor**

[14] "Medical Product Alert N°2/2021: Falsified COVID-19 Vaccine BNT162b2", World Health Organization, March 26, 2021, at: https://www.who.int/news/item/26-03-2021-medical-product-alert-n-2-2021-falsified-covid-19-vaccine-bnt162b2
[15] "How Counterfeit Covid-19 Vaccines And Vaccination Cards Endanger Us All", Judy Stone, Forbes, March 31, 2021, at: https://www.forbes.com/sites/judystone/2021/03/31/how-counterfeit-covid-19-vaccines-and-vaccination-cards-endanger-us-all/?sh=6e4cb3143649
[16] "Operation Stolen Promise – One Year Anniversary", United States Homeland Security at: https://www.ice.gov/topics/operation-stolen-promise
[17] Ibid.
[18] "Beware of Fraudulent Coronavirus Tests, Vaccines, and Treatments", United States Food & Drug Administration, March 1, 2021, at: https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments

social media and online marketplaces promoting and selling fraudulent COVID-19 products.[19] The FDA partnered with the Federal Trade Commission issued warning letters to companies for selling fraudulent COVID-19 products – resulting in seven letters being sent to companies in March 2021.

What is Happening in Canada?

In a recent article from Global News Canada, a reporter registered with an online referral service that connects customers with drug suppliers in India. These **sellers contact those who register immediately over email, text, and social media to offer drugs, often for the treatment of COVID-19, at very low prices.** The reporter received several inquiries from suppliers who offered to sell hydroxychloroquine for a portion of the cost of the price in Canada. [20] Sellers offer to send the products through national postal services with "[c]ustoms cleared (and) home delivery within two weeks or earlier."[21]

During the first six months of the pandemic, there were at least **535 illegal shipments of chloroquine and hydroxychloroquine stopped at the Canadian border**. These shipments were flagged by the Canada Border Services Agency (CBSA) and inspected by Health Canada between March 1st and November 25th, 2020. [22] It is important to note that currently, CBSA and Health Canada **do not have an accurate database to track the total number of illegal medications stopped at the border.**

On December 16th, 2020, Health Canada issued an **advisory warning for Canadians to not buy COVID-19 vaccines being sold online from unauthorized sources.** Health Canada said that the Department "will not hesitate to use all tools at its disposal to stop these illegal activities and will refer incidents of suspected counterfeit COVID-19 vaccines to the Royal Canadian Mounted Police."[23]

As mentioned above, on March 31st, 2021, the Canadian Anti-Fraud Centre (CAFC) issued a warning over the proliferation of scams related to COVID-19 vaccine procurement. **After receiving reports of scams and frauds linked to COVID-19 vaccines,** the CAFC warned Canadians to "not buy COVID-19 vaccines online or from unauthorized sources." [24] The CAFC cautioned of new scams including "coronavirus-themed emails or text messages" attempting to trick people into downloading malicious apps, as well as unsolicited calls from people claiming to represent clinics or private companies that can provide vaccination kits for an upfront fee.

CAFC Findings Between March 6, 2020 and March 31, 2021

- Canadian reports of COVID-19 fraud: 17,005
- Canadian victims of COVID-19 fraud: 15,198
- Lost to COVID-19 fraud: $7.25 M

Source: The Canadian Anti-Fraud Centre

[19] Ibid.
[20] "'Don't worry about it': Dubious online pharmacies push unlicensed COVID-19 treatments", Global News, May 11. 2021, at: https://globalnews.ca/news/7823555/online-pharmacies-unlicensed-covid19-treatments-canada/
[21] Ibid.
[22] Ibid.
[23] "Health Canada warns Canadians not to buy COVID-19 vaccines sold online or from unauthorized sources", Health Canada, December 16, 2020, at: https://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2020/74579a-eng.php
[24] "COVID-19 Fraud", The Canadian Anti-Fraud Centre, March 31, 2021, at: https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

Threat to Canadians

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.[25] The survey revealed **an upward trend of Canadians purchasing medications online** compared to a survey we conducted a couple of years ago and has **remained since ASOP Canada's initial survey conducted in May 2020**. The following are the key findings from the study:

1. As a group, the majority of **Canadians trust in their government's guidance on COVID-19** and are enthusiastic to get the vaccine.
2. T**here are large subgroups of the population who believe COVID-19 is overblown, find online or in person communities more sensible than official government sources, and believe off the shelf or home remedies for COVID-19 both safe and effective.**
3. Most Canadians are open to purchasing medications or medical supplies from an online source, a trend that has increased over the course of COVID-19. Most are open because of perceived convenience and quick access. A concerning **1 in 3 would use an unsanctioned site if it was cheaper or gave access to a desired COVID-19 remedy.**
4. A **significant minority of Canadians have even come across an online source for a COVID-19 remedy that can be ordered online, something younger Canadians (under 30)** have been particularly exposed to. Many agree that if they were ever going to seek an online remedy, they would **select a source that pops up in a search engine.**
5. **1 in 4 Canadians are vaccine hesitant and have a significant trust in the natural health community & natural health products companies on COVID-19 medication advice.**

Young Canadians and COVID-19 Cybercrime

The survey results demonstrated an immediate concern when it comes to young Canadians:

YOUNG CANADIANS (>30)

- 7 in 10 **OPEN TO PURCHASING MEDICATIONS ONLINE.**
- 6 in 10 **FEEL DEPRIORITIZED FOR VACCINATION.**
- 4 in 10 **BELIEVE HOME REMEDIES ARE SAFE & EFFECTIVE.**
- 6 in 20 **HAVE TRUST IN THE NATURAL HEALTH COMMUNITY**.

With **higher COVID-19 rates in young Canadians** and an increase in vaccine hesitancy; younger Canadians **not being prioritized in vaccine rollout plans**; and **increased openness of young Canadians to research and purchase online**, the Government of Canada needs to take an active role in addressing COVID-19 cybercrimes and the threat of COVID-19 vaccines.

[25] This is the second survey in a series. The first survey, conducted in May 2020, can be found at: https://bit.ly/316EgtJ. The results from the second survey, conducted in March 2021 are not yet public, but can be presented upon request.

What Can Be Done?

As demonstrated in the national and international activities above, **a coordinated effort must be adopted that targets the criminal networks and online marketplace of counterfeit vaccines, misinformation, and cybercrime.**

As the global community, particularly the United States, makes progress on the issue of online sales of counterfeit medications and vaccines, **Canada will become a safe haven for criminal networks.** Illegal online sellers will continue to operate in Canada if enforcement gaps continue.

Law Enforcement Gaps	
Mixed Jurisdiction	• Jurisdictions can fall to provincial regulators or federally to Health Canada in case of selling unapproved medicines outside Canada. • If products legitimately counterfeit for sale in Canada, the products fall to RCMP.
Difficult to Build a Case	• Victims of medicine fraud are underreported. • Illegal sellers maintain web of global operations, making it difficult to collect coherent set of evidence.
Limited Incentive to Prosecute Criminals	• Counterfeit crimes not given high degree of priority, even though association to organized crime is clear. • Border officials not evaluated on seizures of counterfeit, substandard medicines.

There are several tools and resources available to the Government of Canada to address issues in online accountability and tackle the public health and public safety threat that illegal online activities create.

Achieving Online Accountability in Canada	
Domain Name Registries and Registrars (R/R)	• **R/Rs required to lock and suspend domain names** when notified by trusted parties providing evidence of content posing threats to public health and safety. • **Establish a third-party notifier program** in Canada to provide an opportunity to R/Rs to take down websites post notification. • Privacy legislation should not complicate law enforcement pursuit of an active investigation: In addition to protecting against bad actors who target online data and create schemes to target companies and databases, the **DCIA should not act as a barrier to law enforcement and government agencies obtaining pertinent personal information** relevant to investigations. • Legislation should require registries and registrars to **provide open access to WHOIS records** that are accurate, non- anonymous and accessible at scale.
Social Media, Online Marketplaces and Search Engines	• **Most U.S. major social media, online marketplace and search engine companies have made commitments to better police illegal online opioid sales in the U.S.**, however similar commitments in Canada are not clear.

	• Search engines must be **encouraged to de-index certain websites selling counterfeit, unapproved COVID products, opioids, controlled substances etc.**
Establishing a Well-Resourced, Centralized and Whole of Government Approach to Tackling Cybercrime	• **Health Canada, RCMP and CBSA lack the authority, tools and/or resources** to monitor and seize counterfeit, unapproved products sold online. • **Local law enforcement services lack the incentives or resources** to pursue crimes. • **Centralized government program**, either expanded under Canadian Anti-Fraud Centre or new entity such as U.S. IPR Center Technology, tools, trained personnel to collect evidence for enforcement community as a whole. • Address **barriers to investigations** by working with RCMP, CBSA, Health Canada, local law enforcement. • **Centralized program with authority to coordinate** tools available to hold bad actors accountable (administrative, tax, law enforcement).
Including the Online Sale of Illicit and Counterfeit Drugs in Online Harm and Web Regulation Legislation	• Without the inclusion of the online sale of illicit drugs in upcoming legislation that deals with online harm and the regulation of the web, the Government is **creating a loophole for criminal networks to continue public health and public safety.** • By including illegal activity in online harm and web regulation legislation, **criminal networks will not be able to expand into future public health crisis**.

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.

ASOP Canada would like to thank the members of the Standing Committee on Health for the opportunity to submit this briefing. We would like to offer our organization, members, and network of experts as a resource to the Committee with regards to COVID-19 cybercrime and counterfeit vaccines.