

PROTECTING AMERICANS FROM DANGEROUS FAKE & FRAUDULENT COVID-19 PRODUCTS SOLD ONLINE

THE ISSUE: Criminals have long exploited enforcement blind spots online to sell fake and fraudulent products, but COVID-19 has created new opportunities for these bad actors to take advantage of consumers' confusion and fears, ultimately putting lives on the line. At the outset of the pandemic, there was a rapid proliferation of thousands of websites peddling fake COVID-19 "cures," each trying to profit by preying on consumers' false hopes. Now, as demand for COVID-19 vaccines increases and each state adopts its own distribution system, Americans are relying on the internet for information on how and where to access a vaccine. At the same time, criminals lurk online to capitalize on the crisis.

Illegal Online Drug Sellers Have Long Put Public Health at Risk for Profit

- At any given time, [96% of the roughly 35,000 online pharmacies worldwide](#) operate illegally, in violation of state and/or federal law and pharmacy practice standards.
- These sites [threaten American lives](#) by selling medicines without a prescription, operating without a license, and peddling counterfeit drugs and miracle treatments, often containing dangerous – even deadly—ingredients like paint thinner, fentanyl, mercury, and tar.
- Worth [\\$200 billion a year](#), the market for counterfeit pharmaceuticals now eclipses almost everything else in the underground economy, including prostitution, human trafficking, and illegal arms sales.

The Pandemic is Making It Worse

First-time online drug purchasers increased in 2020, but many are unaware of risks:

- The growing demand for health care delivered virtually and more convenient, lower-cost medications has been accelerated by the COVID-19 pandemic: [31% of consumers who have bought prescription medication online](#) did so for the first time in 2020, driven by the pandemic.
- [More than one-third of Americans have used an online pharmacy to buy medicines](#) for themselves or someone in their care – up from just 1 in 4 from a 2013 survey by the U.S. Food and Drug Administration.
- [Half of Americans](#) would consider purchasing medication online for everything from medicines for chronic conditions to COVID-related products like vaccines. As states roll out COVID-19 vaccinations, consumers turn to the internet for information about how and where to get a vaccine – creating more opportunities for cyber criminals to target unsuspecting individuals with misinformation, fraud, and fakes.
- This is a huge problem because [large numbers of consumers](#) misunderstand or underestimate the risk of illegal online pharmacies:
 - 37% see little risk in ordering from one, while 7 in 10 Americans incorrectly believe that if a website appears higher in search results, it is likely to be legitimate.
 - And 4 in 10 Americans erroneously believe that all websites offering healthcare services and/or prescription medications via the internet have FDA or state regulator sign off.

Online criminals are capitalizing on high demand for COVID-19 products to turn a profit at the expense of consumers' health and wealth:

- In March 2020 alone, [tens of thousands of websites](#) were registered with terms like "COVID," "corona" and "virus," [90% of which were registered anonymously](#). Many websites have since been activated to defraud patients, including the sale of unapproved COVID-19 treatments and vaccines.
- In [March 2020, a U.S. Federal Court issued a temporary restraining order against a website offering COVID vaccines](#). The legal complaint's target was the domain CORONAVIRUSMEDICALKIT.COM, the operator of which was selling non-existent coronavirus vaccine kits.
- In November 2020, the U.S. Immigration and Customs Enforcement (ICE) announced the [launch of Operation Stolen Promise 2.0](#) targeting COVID-19 vaccine fraud. This follows on the success of Operation Stolen Promise 1.0, which was focused on the pandemic and broader sale of counterfeit or substandard products and related financial fraud.
- In December 2020, the [U.S. Attorney for the District of Maryland seized](#) two domain names, *mordernatx.com* and *regeneronmedicals.com*, which duped would-be customers into providing personal information by replicating the websites of COVID-19 vaccine and treatment manufacturers.
- On January 22, 2021, following FDA action, the [US DOJ arrested a criminal for illegally offering unapproved COVID-19 vaccines online](#).

Public Awareness and No-Cost Policy Solutions Can Help Keep Americans Safe

- [FDA's investigations into fraudulent COVID-19 treatments](#), as well as warning letters from the agency, are an essential step in protecting Americans from COVID-19 related scams and counterfeit products, but more can and must be done.
- [The Alliance for Safe Online Pharmacies](#) (ASOP Global) and its members are working to raise awareness about the safety and availability of legitimate COVID-19 vaccines and educate consumers about the risks of fraudulent COVID-19 products being sold online.
- ASOP Global advocates enacting and enforcing [bipartisan no-cost policies to create a more transparent and accountable internet](#), including:
 - Restoring access to accurate [WHOIS data](#) to ensure that the FDA, law enforcement, cybersecurity, and other stakeholders have access to contacts for websites and domain names to aid in their investigations.
 - Requiring domain name registries and registrars to [lock and suspend](#) suspicious sites upon notice from a trusted notifier, such as the FDA. The FDA and NTIA just completed a [successful pilot](#) of the trusted notifier model, which led to the takedown of nearly 30 illegal pharmacies online.
 - Targeting reforms to Section 230 of the Communications Decency Act that require companies to report suspicious online activity to law enforcement and take other reasonable steps to prevent this unlawful activity.