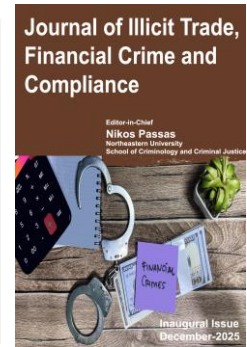


Journal of Illicit Trade, Financial Crime, and Compliance

ISSN (online): 3070-6122



Illicit Online Pharmacies (IOPs), Counterfeit Medicines, and the Enabling Financial Ecosystem

Layla Hashemi^{1,*}, Louise Shelley² and Edward Huang³

¹*Women In International Security (WIIS), Washington, DC, USA*

²*Distinguished University Professor Emerita, George Mason University, Arlington, Va., USA*

³*Samuel Ginn College of Engineering, Auburn University, Auburn, Alabama, USA*

ARTICLE INFO

Article Type: Research Article

Keywords:

Illicit online pharmacies

Counterfeits

Harmful pharmaceuticals

Cryptocurrency

Illicit financial flows

COVID-19.

Transnational crime

Timeline:

Received: May 23, 2026

Accepted: July 05, 2026

Published: July 13, 2026

Citation: Hashemi L, Shelley L, Huang E. Illicit Online Pharmacies (IOPs), Counterfeit Medicines, and the Enabling Financial Ecosystem. *J Illicit Trade Financ Crime Compli.* 2026; 2: 62-74.

DOI: <https://doi.org/10.65879/3070-6122.2026.2.05>

*Corresponding Author

Email: laymay.19@gmail.com

ABSTRACT

A sharp rise in illicit online pharmacies (IOPs) over the last decade poses significant threats to public health and safety because the unregulated medicines sold are often of inferior quality with no active ingredients or contain harmful chemicals. American consumers provide a major market for online pharmacies, of which 95% operate with flagrant disregard for the law [1, 2]. This article is based on research conducted by the authors analyzing hundreds of online pharmacies, with particular attention to the payment methods used by IOPs, a problem not previously examined in depth in other studies of online pharmacies. The research concluded that the predominant payment method was cryptocurrency, followed by credit cards and third-party payment processors. Use of cryptocurrency on a significant scale is often indicative of financial crime. We observed significant growth of illicit activity during the pandemic and IOPs followed the same trend as customers turned increasingly to online platforms for all forms of purchases. Unfortunately, the problem of dangerous and substandard medicines sold through IOPs continues on a massive scale in the post-pandemic era. New and dangerous products have joined the offerings initially studied, including counterfeit oncology drugs, weight loss drugs, and other newly developed medicines added to the profiles of IOPs. Therefore, IOPs are an increasingly pervasive form of illicit trade undermining human, national, and international security as well as intellectual property rights, and are often facilitated by an unaware and sometimes complicit financial community.

©2026 Hashemi *et al.* Published by Journal of Illicit Trade, Financial Crime, and Compliance. This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited. (<http://creativecommons.org/licenses/by-nc/4.0/>)

¹This research work was supported by the National Science Foundation in the United States under Award D-ISN-2039779: Collaborative Research: An Interdisciplinary Approach to Understanding, Modeling, and Disrupting Drug and Counterfeit Illicit Supply Chains.

1. Introduction

The entry of counterfeit medicines into global supply chains is a serious problem, but their penetration occurs through different methods in different parts of the world. In developing countries in Africa, as well as in other regions of the less economically developed world, corruption is a major facilitator of the entry of counterfeit and inferior drugs into the market [29]. In these areas where regulation is weak, there are limited controls and facilitation payments come directly from the sellers of inferior and counterfeit drugs into the marketplace. INTERPOL has run numerous coordinated seizures of massive amounts of counterfeit drugs through its Pangea operations. In the 16th iteration of Pangea between December 2024 and May 2025, 123 criminal groups worldwide were dismantled as an INTERPOL-coordinated operation across 90 countries, resulting in the seizure of 50.4 million doses of illicit pharmaceuticals worth USD 65 million [4].

Online marketplaces have facilitated the entry of some of these illicit medicines as the Pangea XVI announcement points out, but the sale of medical drugs through online platforms is a particular problem of the developed world. The data that form the basis for this study consist primarily of information from websites that target the US customer base because of the great demand for affordable medicines. But there is also extensive documentation of the entry of counterfeit and inferior medicines by means of online platforms to other developed countries [5]. The actors behind IOPs are often criminal networks less reliant on corruption than the purveyors of counterfeit drugs in Africa and elsewhere, where local officials may be bribed by pharmaceutical companies to ensure the distribution of their goods [6], as well as by counterfeit sellers who distribute inferior goods in marketplaces and through pharmacies.

This article particularly focuses on online illicit marketplaces that target American consumers as they are the largest online purchasers. The United States is the main consumer for online pharmacies, representing the highest proportion of traffic to both legal online providers (97%) and IOPs (60%) among all countries [3]. IOPs, many allegedly operating out of Canada [7], now dominate the market for online medicines in the United States and are accessed in other countries to a lesser degree [8, 9, 10]. The absence of affordable insurance for medicines and the high cost of prescription drugs means that many Americans turn to IOPs that offer medicines at more affordable prices for many different illnesses such as diabetes and cancer, hypertension, including diverse oncology drugs, insulin, and mental health prescriptions. The high proportion of US consumers relative to online purchasers was also observed by McCoy, Krebs and others in their examination of the spam that directed customers to illicit pharmaceutical affiliate networks (and other illicit supply chains) that provided access to drugs of choice such as Viagra. Based on customer shipping addresses, McCoy *et al.* determined that across GlavMed and SpamIt programs, customers from the United States dominated 75% of orders, with Canada, Australia, and populous countries in Western Europe following in single digits [11]. This has also been identified by the EU Intellectual Property Agency as a problem in European countries. Recent research in the UK by a governmental agency reveals that online purchases with cryptocurrency have become a problem there as well [13].

"Illicit online pharmacies (IOPs, also known as illegal, illegitimate or rogue online pharmacies) are websites that violate regulations by selling counterfeit, adulterated or unapproved drugs or dispense prescription drugs without a valid prescription. IOPs do not meet national or international pharmacy regulations, nor have IOPs been subjected to the requisite regulatory review, licensure and/or certification." [1]. These often-harmful purveyors of pharmaceuticals now represent 95% of online pharmaceutical drug sales. Most are deceptive, often including photographs of doctors and medical personnel to give them an air of legitimacy [1]. They offer purchasers medicines, often at highly competitive prices, and most consumers are not aware that they may be buying an inferior or even dangerous counterfeit product, or one transported under inappropriate conditions with no concern for temperature control or other required transport procedures. The patients' ignorance is compounded by the fact that many doctors are incapable of identifying harmful online providers for their customers [9].

The products purchased through IOPs can have harmful and even deadly consequences [41] as they may be selling products with no active pharmaceutical ingredient (API) or less API than would be present in an authentic product. Some IOPs may be selling diverted authentic goods which may have been improperly handled, transported, or stored. They may also offer products that have expired. In the worst cases, these medicines may have deadly

elements such as fentanyl or harmful non-addictive chemicals added to their product [15]. The products on these sites are not associated with and monitored by established and reputable, or licit, pharmaceutical companies such as Walgreens or other known licit online pharmaceutical distributors. Vendors/sellers also try to mimic or impersonate the websites of known brands such as Walgreens. This increases the possibility that an unsophisticated consumer will be exposed to inferior or dangerous products to treat diverse diseases where the substitution of these low-quality drugs or harmful counterfeit drugs without any or minimal actual active ingredients may result in dangerous side effects or life-threatening consequences [14].

China, Hong Kong, and India have been identified as the source of many of the products, or the precursor chemicals for products, sold on IOPs [16]. Many pharmaceuticals sold on the IOP market are produced by companies in India that specialize in generics [17]. Turkey has also recently entered into the market as a seller of counterfeit oncology drugs as well as drugs for life-threatening conditions [18, 19]. These countries have much more lax regulation of their chemical and pharmaceutical industries and domestic corruption may contribute to their global distribution. Sometimes, the products sold on IOPs are produced during third shifts of generic producers [16].

The Census Bureau's Annual Retail Trade Survey (ARTS) reported that e-commerce sales increased by \$244.2 billion or 43% in 2020, the first year of the pandemic, rising from \$571.2 billion in 2019 to \$815.4 billion in 2020 [22]. The lockdowns of many distributors of pharmaceuticals and the disruption of supply chains during the COVID-19 pandemic, also contributed to a sharp rise in online purchases of medicine and other health products including safety equipment such as medical masks. During the COVID-19 pandemic, customers also looked for Ivermectin, a parasite drug, as well as other medicines that were touted as a COVID-19 treatment but were not approved by US government agencies for treatment [23] sending some consumers to online marketplaces where these products were advertised. Enhancing the risk of engaging with these marketplaces was that corruption undermined the integrity of supply chains [20] as shortages of needed goods reduced oversight, thereby increasing the availability of falsified and substandard products [21]. At the same time that quality controls went down, purchases went up.

In addition to the increase in online trade, consumers were also less likely to conduct proper due diligence and research into the authenticity of products, including medicines, due to supply chain disruptions and the lack of availability of products. Some IOPs employ deceptive practices such as displaying images of medical professionals, professional profiles, official trademarks, and various forms of publicly available information to create an appearance of legitimacy, thereby making it more difficult for consumers to distinguish between legitimate and illegitimate internet pharmacies [44]. Also, a large percentage of doctors surveyed were found unable to help their patients differentiate between a legitimate provider of drugs and a website that might place them at risk of acquiring counterfeit medicines. These factors led to an even more dangerous pharmaceutical market in which IOPs capitalized on the chaos of the COVID-19 pandemic to enter their illicit products into legitimate supply chains [1][9].

Tracking and disrupting IOP websites presents substantial challenges. Many webpages serve primarily as entry points designed to attract customers and function as promotional or advertisement portals. In contrast, the webpages used for browsing and purchasing counterfeit medicines are often developed as modular software components, allowing operators to rapidly redeploy them across multiple domain names and hosting servers. Data collection and investigative efforts indicate that website takedown strategies are frequently ineffective, as operators can acquire a new domain name for approximately \$300 and redeploy a replacement website within minutes. Payment webpages, however, are typically facilitated by third-party payment service providers. Consequently, tracing payment portals and associated financial channels may offer a more effective avenue for disrupting IOP operations than traditional website takedown approaches. This is key as we are dealing with a form of financial crime selling needed medical goods of dangerous or inferior quality, often by means of cryptocurrency closely associated with criminal networks [30].

Most existing literature on illicit online pharmacies [24] focuses on specific aspects of the problem such as public health and safety, policy and regulation, marketing and law enforcement issues [21]. There has been much attention to the sale of counterfeits in both the developing world and in online marketplaces. There has, however, been limited attention paid by the academic literature to the financial payments associated with IOPs, which is the focus of this article.

Following the money is key because law enforcement has long discovered that one of the major ways of incapacitating illicit actors is to deprive them of their revenues. Furthermore, the platforms that host the IOPs are not sufficiently vigilant in addressing the identity and intentions of the sellers who use them. Therefore, to successfully disrupt IOPs, it is necessary to understand how they receive payments from customers. The existing literature on illicit supply chains notes that this illicit activity needs facilitators from the legitimate economy to operate [25]. The most common form of payment advertised for IOP purchases are cryptocurrencies, particularly bitcoin, but trade is also facilitated by a variety of actors from the more established legitimate economy including credit card providers and wire transfers of financial institutions. Third-party payment processors such as PayPal and Venmo also facilitate payments for online purchases in the US, thereby allowing harmful and dangerous products to cross borders. In the UK, PayPal does not allow these purchases [27][28][24][29].

Unfortunately, as our research reveals, IOPs are skillful in obfuscating their revenues and financial flows, making it harder to disrupt and limit their illicit trade [26]. As they have increasingly used cryptocurrencies for payments, the financial flows are harder to detect, sanction sellers, or recover funds obtained from the sale of illicit products. Even if the owners of the wallets can be determined after investigations, the money may have already been transferred to jurisdictions where the funds cannot be recovered and only limited funds may be recovered from identified wallets [12].

The monitoring of these illicit sellers is undermined by the illicit traders' ingenuity in circumventing controls. While international bodies such as The Internet Corporation for Assigned Names and Numbers (ICANN) and domain registrars adhere and respond to filed abuse notices, this reactive process only addresses currently active domains by suspending accounts. As a result, many IOPs adhere to a common business model. They easily re-establish their businesses online after removal. This leads to what some experts call the "whack-a-mole" problem once a website or domain is taken down for illicit activity, they simply pop back up under a different name or account and become the registered owner. While regaining access to merchant accounts can also be time consuming, even high-risk merchant accounts can be re-established within a few days.

2. Methods

IOP data collection ran from January 2021- July 2023, slightly after the World Health Organization (WHO) determined the end of the COVID-19 pandemic in May 2023 [37]. The last payments collection date used for this article was July 2023, although the authors have kept up with the trends identified in the online payment community.

This research expanded and complemented the work we were doing on counterfeit medical masks intended for health care workers and emergency providers, which began intensively in February 2021. Almost all of these masks were also sold online but through different websites than the ones analyzed in reference to medicines sold through IOPs. In this way, we could expand our analyses of the consequences of the pandemic on diverse health products in the e-commerce space.

The data collected on counterfeit medical masks was conducted in cooperation with 3M company, and we were able to collect large amounts of data as complaints were made concerning the delivery of substandard products and seizures were made internationally. Likewise, we were able to secure the support of Legit Script, a leading risk compliance company in the pharmaceutical sector. The initial data collection was done through collaboration with Legit Script and other specialists in illegal online medical sales. These subject matter experts provided background and historical knowledge on the IOP trade and helped guide the collection and analysis of emerging patterns and trends during the COVID-19 pandemic. They also helped to understand the attributes of IOPs. This helped the authors, assisted by NSF-funded undergraduate researchers, to collect over 1,000 domains, although only around 860 domains were determined to be advertising illicit pharmaceuticals after consultations with our Legit Script partner and other risk specialists in the pharmaceutical health sector. Our identification of IOPs evolved over time. Initially, we did a bulk search with Legit Script and Domain Tools that was conducted using keyword and domain searches, but this led to some original domains that had been identified as problematic and had been blocked, suspended, parked, or shut down. But this bulk analysis was not always useful to understand financial flows as some of the 860 identified sites lacked payment information.

Therefore, to focus more on illicit financial flows, we narrowed our analysis to the 407 websites that were visible online from the start of the pandemic. This did not preclude the fact that they might be linked to other IOPs that were operational before the pandemic. Examining IOPs in the pre-pandemic period revealed that there were important similarities in the online presentations of pre- and post-pandemic era IOPs, suggesting the continuity of IOPs by the same owners. But continuity of illicit operators in the IOP space was not analyzed as it was outside the primary focus of this analysis understanding the money flows of IOPs during the pandemic.

Over time, we refined our detection capacity and focused only on IOPs that were active during the pandemic. Among the websites active during the pandemic, some had been established earlier and may have existed as early as 2016 or earlier, changing owners or hosts over time. Others entered the marketplace only after the start of the pandemic. We then identified whether the domain was a licit or illicit online pharmacy based on a variety of factors including analysis of product descriptions, domain data and terms of service, company policies and information, as well as other publicly available content such as images or identifying information.

Once an IOP domain was identified as an IOP, we used a variety of open-source or publicly available information and domain analysis to find related or linked domains. The purpose of this analysis was to determine whether the same company was using different online platforms to market its products. Indicators of common or related ownership structures included, for example, similar emails, phone numbers and other attributes such as the use of the same stock images. This research technique was also used in our identification of counterfeit medical masks [34], as well as in subsequent research on the detection of fentanyl producers [35].

Key to our data collection for this project, in contrast with the fentanyl and counterfeit mask projects, was the analysis of payment information. This payment information revealed the involvement of diverse legitimate companies' payment providers as IOPs sought to maintain an image of legitimacy, often identifying themselves as Canadian or other falsely located pharmacies.

All 407 domains analyzed were examined to determine the types of financial payment methods that were accepted, such as Cryptocurrency, Credit Card, Third Party (or peer-to-peer (P2P)) Payment Processing, Money Transfer, Bank Transfer, and Gift Cards. Examples of subcategories of the above payment types include but are not limited to: Cryptocurrency (Bitcoin, Ethereum); Credit Card (Visa, Mastercard, American Express); Third Party (PayPal, Venmo, Cash App). The sampling for domains was not random, but rather based on those domains that explicitly advertised payment methods, a limitation which could potentially product selection bias towards those websites that have more payment method transparency. However, this study was designed to examine observable payment ecosystems rather than estimate the prevalence of all IOP payment behaviors across the broader online marketplace. Despite the value in identifying accepted payment methods by IOPs, another limitation worth noting is the inability to observe what payment methods are actually used or if transactions are completed successfully either generally or for specific payment methods. The breakdown of these payment methods will be discussed in the following section on results.

3. Results

This section provides an overview of IOP payment patterns revealing a key element of the business model of these illicit pharmacies. It then takes a deep dive into payment methods used by customers. Given the large number of websites that offered sales through bitcoin, not a traditional payment method on websites for medicines, there should have been greater concern among buyers as to the reliability of the sellers. Analysis by Chainalysis in 2024 has shown that many counterfeit medical producers listing their products online accept crypto as well as more conventional payment types. In many cases, it is unclear whether pharmaceutical shops are selling legitimate products diverted from the legal supply chain or generic medical products branded as legitimate. Regardless, actors selling these products in exchange for crypto are harming the intellectual property rights of legitimate pharmaceutical companies [12].

It should be noted here that though the data collection for this study was conducted during 2021-2023 and the cryptocurrency ecosystem has evolved in terms of payment technologies and enforcement mechanisms. More recent public reporting by organizations such as Chainalysis, INTERPOL, Europol, and regulatory agencies

acknowledges these evolving payment technologies and enforcement mechanisms but remains consistent with the broader patterns identified in our analysis. Although we acknowledge the time gap, we believe this study remains a meaningful contribution to the literature based on the timeframe in which the data were collected.

The more recent insights demonstrate the continued relevance of the trends identified in our dataset, particularly the persistence of cryptocurrency for criminal use, decentralized payment mechanisms, and evolving regulatory responses. Unfortunately, there has been an absence of a coordinated transnational response to abuses by criminals of cryptocurrency or a collaborative legal response between the United States and Europe as there are now fundamental differences because the United States legal system has eschewed a commitment.

Eighty percent of the over 400 identified IOPs with associated payment data accepted cryptocurrencies. A lesser number accepted credit cards (48.5%), third-party payments (43.8%), money transfers (30%), bank transfers (14.6%), and gift cards (12.9%) as a form of payment, as shown in Figure 1 below. This reveals the centrality of cryptocurrency in illicit marketplaces and in IOPs in particular, a finding that establishes common financial attributes with e-commerce for other forms of illicit activity such as narcotics and child sexual material [30]. According to Chainalysis, a major firm in the cryptocurrency analytics field, cryptocurrency is most frequently used for sanctions evasion. Although IOPs are a small share of the cryptocurrency market today the illicit pharmacy market is dominated by the use of Bitcoin, there is pernicious use for this form of cryptocurrency. This form of payment is not generally associated with legitimate online pharmaceuticals. For example, such widely used online platforms as Walgreens rely on credit card payments and have no possibility of using Bitcoin as a payment method.

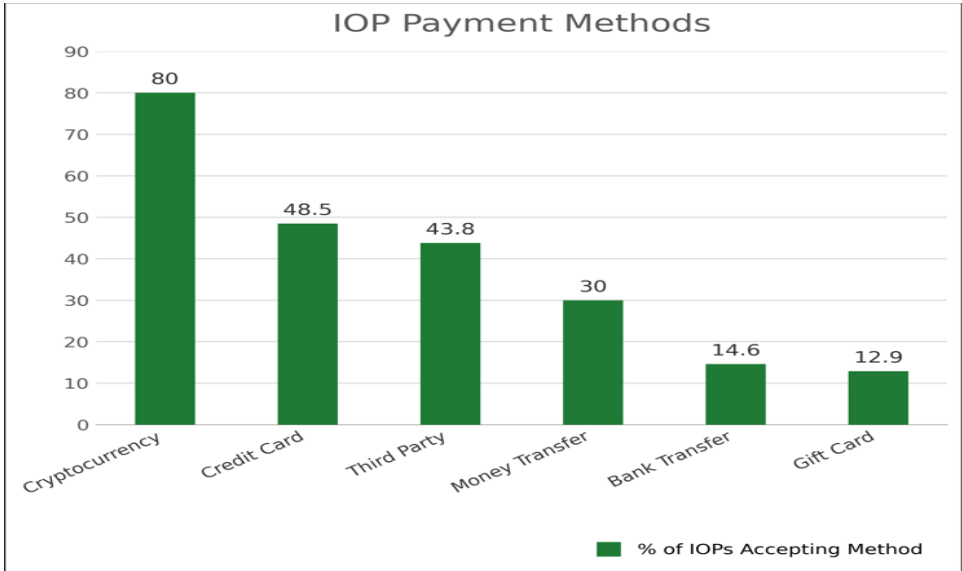


Figure 1: IOP Payment Methods Overview.

The data analysis reveals that over 65% of the transactions involve banks through credit cards and bank transfers. The 65% figure refers to the proportion of analyzed domains advertising payment mechanisms involving traditional banking infrastructure, including credit card systems and bank transfers, rather than estimated transaction volume. This shows that legitimate financial institutions such as banks are key contributors to the purchase of possibly dangerous pharmaceuticals. It suggests that there should be much more analysis by the banking sector of the charges made to their credit cards as well as the bank transfers, they process.

Credit card payments have a variety of benefits, perhaps most importantly that most consumers (especially in the developed world) own a credit card and thus can make this form of payment quickly and easily. Approximately 21% of the world uses credit cards, but these numbers are as high as 83% in Canada, which is a hosting center of IOPs [32]. Despite these benefits, credit card merchant accounts are difficult to set up for IOPs. To gain access to credit card payments, IOPs must essentially work around the system to gain access to credit card payments through third-party payment processors. This is because many of the major payment processors or aggregator platforms classify pharmacies as prohibited or restricted businesses due to regulatory complexity, chargeback risk and

reputational concerns [26]. Once established, it is likely that the merchant account will be shut down or suspended at some point and again after re-establishment, making this a convenient but risky payment method for IOPs. It is worth noting that while all vendors are at risk of chargebacks or a reversal of payment when accepting credit cards as a method of payment, this is unlikely to be the case for IOPs unless they are non-delivery scams which do not provide actual product after making a transaction. Corruption within the financial sector, especially in countries with less regulated markets, can also facilitate payments by moving illicit funds through legitimate institutions such as banks, credit card companies, and third-party payment processors [11].

Finally, a few of the benefits of third-party processors are ease of setup and popularity. IOPs experience less friction in getting service established through third parties than through alternative payment methods such as credit cards or bank transfers. Additionally, third-party payments are becoming increasingly more popular and are easily integrated into the domain's website. The most common third-party payment processors used by IOPs are PayPal, Venmo, and CashApp. PayPal owns Venmo and accounts for 22% of all online transactions in the US [40]. While there are many benefits to using third-party payment processors, there are also costs for their convenience. Many charge a fee for processing and third-party payments can also be traced and disrupted by police and other enforcement entities.

Based on the data in Table 1 below, over 80% of stand-alone domains accept two or more payment methods, while only approximately 19% accept only one form of payment. These findings demonstrate how vendors rarely rely on only one form of payment, likely as a precaution against having their accounts suspended, blocked, or seized. They diversify payment methods to reduce risk.

Table 1: Number of Payment Methods by Domain (Stand-Alone and Connected).

Number of Methods	Stand-Alone	Connected
1	19%	14%
2	44%	35%
3	31%	42%
4	4%	8%
5	1%	2%

Research was conducted on the connections among the IOP sellers suggesting that many were linked in ownership, or companies of illicit sellers had many diverse platforms. Connected networks were determined by identifying at least two links between domains. Indicators of network connections include shared IP address, email address, phone number, website template, MX server, or other shared information. Once two of these links were identified and confirmed, the domain was then categorized as being connected. Network determination was primarily determined by analyzing domain name service (DNS) data through a variety of methods and tools, including Domain Tools, a commercially available product suite including Domain Tools Iris, the company's comprehensive threat intelligence and investigation platform designed to help analysts and investigators identify, track, and analyze malicious infrastructure. For example, analysis allowed us to determine the registrant (domain owner), phone number, email address, IP address, and other important information that could help establish links with other domains. It should be noted here that sometimes this information is unavailable, redacted for privacy, or strategically falsified to obfuscate IOP activity. As shown through studies such as Altana's Atlas [33], the redundancy of these illicit networks exists in the ecosystems of other illicit marketplaces including the dark web trade of drugs as well as human trafficking supply chains. The authors also processed the data by removing all known connected networks and retaining known and newly connected networks. As a result of cleaning and refining the data and removing duplicates, we had a subset of 161 stand-alone domains and 60 networked domains, a total of 221 domains for which we conducted more in-depth payment analysis.

Table 2 provides an overview of Payment Methods accepted by Connection Category measured in percentage. Because sellers accept more than one payment method, the sum of each column totals over 100%.

Table 2: Payment by Connection Category (Percentage).

Methods	Stand-Alone (N=161)	Connected (N=60)
Credit Card	24.84	64.20
Third Party	61.49	32.10
Cryptocurrency	88.20	75.31
Money Transfer	33.48	40.00
Bank Transfer	13.12	30.00

Based on data in Table 2, over 88% of stand-alone domains accept cryptocurrency as a payment method, and a slightly lower percentage of connected domains (75.31%) accept cryptocurrency, demonstrating the high percentage of IOPs that accept cryptocurrency as a key, though not exclusive, accepted payment method for products and/or services. This is consistent with findings by Chainalysis on the centrality of cryptocurrency as an IOP payment method [31]. Stand-alone domains (61.49%) accept third-party payments at a higher rate, while connected domains tend to accept more credit card payments (64.20%). Both stand-alone and connected domains also accept money transfers (33.48% and 40.00%, respectively).

Based on the data, connected domains did not commonly combine direct credit card acceptance with cryptocurrency payments. The authors also note that connected networks may rely more heavily on layered third-party processors and distributed payment structures to reduce exposure to merchant account disruptions and compliance monitoring.

The use or acceptance of multiple payment methods provides IOPs the broadest possible customer base to buy their products. The high percentage of payment option overlap between stand-alone and connected domains suggests that there is a standard *modus operandi* for IOP preferred payment methods.

Table 3: Combined Two-Payment Methods by Connection Category (Percentage).

Methods	Stand-Alone	Connected
Credit Card + Crypto	5.8	0
Cryptocurrency + 3rd Party	35.3	48.33
3rd Party + Credit Card	1.38	3.33

Based on the data in Table 3, only 5.8% of stand-alone domains accept both credit cards and cryptocurrency. In contrast, and interestingly, none of the connected domains accepted this payment method combination. As the most common payment combination, approximately 35.3% of stand-alone domains and 48.33% of connected domains accept a combination of cryptocurrency and third-party payments. The authors also analyzed websites for the combined use of three or more payments. While cryptocurrencies, money transfer, and third-party payments were the most commonly accepted payment methods by IOPs, these percentages were relatively low compared to those reported in Table 3, as only approximately 10% of IOP sellers used three or more payment methods.

As shown in Table 4, each payment method entails specific benefits and risks or costs for IOPs. Given the illicit nature of their activity, IOPs must balance maximizing profits while also minimizing risk of detection and disruption.

Table 4: Cost-Benefit Analysis of IOP Payment Methods.

Method	Benefits	Costs/Risks
Crypto	Less risk of detection/disruption	Requires technical knowledge
Credit Card	Readily available	Difficult to establish merchant account; risk of shut down
Third-Party Processor	Ease of set up, frictionless, popular	Significant associated fees; can be shut down

One benefit of accepting cryptocurrencies as a payment method is that there is often less risk of detection and disruption for IOPs, though cryptocurrency transactions and wallets can be tracked [36]. A disadvantage of accepting cryptocurrencies is that this payment method requires a particular level of experience or technical skill on behalf of both the vendor and buyer. While the necessary level of technical skill for crypto transfers can be a challenge, most IOP vendors are able to establish crypto wallets and complete crypto payments due to their consistent involvement in illicit trade.

Companies such as Chainalysis have developed the capacity to monitor the cryptocurrency payments used by IOPs. The Medical and Healthcare Products Regulatory Agency in the UK (MHRA) monitored online purchases of pharmaceuticals and made four test purchases [12]. This provided MHRA with addresses operated by the actors running the shop. Once these actors received MHRA's payments, they transferred the funds to several intermediary addresses. Eventually, the funds reached a mainstream exchange, which likely represents the cash-out point for the operator of the online pharmacy. The intermediary addresses also received funds from addresses that behave in the same fashion as MHRA's target and are likely other services that are part of the same malicious group. Upon completion of these test transactions, MHRA discovered that the actors had transferred millions of dollars to the same mainstream exchange, some but not all of which likely came from the sale of illicit medicines [12]. There are many more jurisdictions that are using the analytics that Chainalysis and other similar companies provide. Unfortunately, as diverse panels at the OECD anti-corruption week conference in March 2026 revealed, that there are increasing difficulties in putting together cooperative investigations between the United States and European countries.

Based on this study of the payment method data connected with the IOPs, a key takeaway is that most IOP vendors will accept credit cards where possible. But keeping merchant accounts open is difficult when illicit activity is often detected and disrupted. Because of the risk of account shutdown, IOPs use multiple (two or more) payment methods while offering credit card payments when possible. While establishing and maintaining an illicit merchant account can be time consuming, risky, and difficult, IOPs that accept credit cards are often able to conduct larger volumes of business due to the widespread use of credit cards, especially in North America (e.g., Canada and the United States). Because credit card merchant accounts are difficult to maintain by IOPs, many vendors, especially those who are newly established or not connected, commonly use third-party payments, an increasingly popular payment method. This shift from the slower money transfer process in the past to the faster third-party, credit card, and cryptocurrency payments represents a continuing trend in the illicit pharmaceutical trade and adds increased rapidity and convenience for purchasers. Therefore, those seeking to combat IOPs need to understand and follow the latest and fastest forms of financial payments if they seek to disrupt these dangerous supply chains.

4. Conclusions

This study, by focusing on following the money in relation to IOPs, offers a different perspective on the problem. The research analysis shows that following the money and payment methods of IOPs sets them apart fundamentally from legal online providers (LOPs). LOPs are committed to preventing counterfeits from entering their platforms and ensure that readily traceable forms of payment are used by purchasers. As our research shows, in contrast, 80% of IOPs offer payment in digital currencies such as bitcoin that require special skills to unravel the source and destination of the money.

The IOPs are often part of diversified criminal networks, as an examination of the accounts associated with bitcoin payments from the UK medical service has shown. As part of the ecosystem of counterfeits, the production and sale of these products may be tied to forced labor as well as other forms of illicit activity [38].

The illicit trade in pharmaceuticals and counterfeit medical supplies is becoming an increasing concern for multinational organizations as it has such important implications for health as well as national, international, and economic security [38]. Vast investments in research and development of lifesaving drugs may be compromised as harmful side effects are reported from their use. But these side effects are not the result of the use of legitimate product, but rather from the infiltration of counterfeit and harmful products into the legitimate supply chain. In the absence of the recognition that counterfeit and diverted medicines may have been prescribed, the medicines may be discredited in medical records. Therefore, the existence of IOPs that facilitate the entry of low-quality or harmful

products provides another challenge for pharmacovigilance that is outside the usual skills of the pharmaceutical industry. But after the investment of sometimes billions of dollars over years through research and clinical trials to develop medicines that can extend lives or even cure patients, this work is undone by the illicit economy that facilitates the entry of dangerous and illicit medicines into legitimate supply chains. The consequences are multifaceted, including great negative costs for human lives as well as pharmaceutical innovation.

As this article has shown, combatting the problem of IOPs requires the application of AI and large-scale data analytics. There needs to be constant vigilance in detecting IOPs advertising and selling harmful medicines and ensuring that they are taken down and are not readily replaced by an alternative webpage where future customers can be deceived. But INTERPOL's efforts through Pangea to stem online sales of inferior medicines remain sporadic and not sustained, whereas the problem, as the research has shown, needs constant vigilance if harmful and inferior medicines are to be identified and removed from supply chains. The problem of fighting IOPs is not just one of resources but one of successful and sustainable efforts to combat the problem long term. There also needs to be much more attention to the analytics behind the cryptocurrencies and other payment methods that are at the core of IOP business models, to prevent money flowing to illicit actors and to ensure that funding for illicit medicines does not flow into and intersect with other forms of illicit trade.

Some researchers have suggested that blockchain analytics may be helpful in ensuring the security of medicines reaching patients [39]. This may prove a useful tool in securing the medicines and their supply chains, but it is not a sustainable solution in the face of a large global criminal ecosystem for which this article has only provided a brief introduction.

Unfortunately, the present divergence of compliance standards between the United States, Europe and other countries makes it more difficult to develop effective national and international policies of accountability.

Recommendations to address IOPs include strengthening the role of financial institutions and payment intermediaries within AML/CFT and law enforcement ecosystems, including banks, card networks, payment processors, fintech platforms, and cryptocurrency exchanges as key gatekeepers capable of identifying and disrupting illicit online pharmacy (IOP)-related financial flows. This includes compliance-oriented practices such as enhanced transaction monitoring, merchant onboarding controls, enhanced due diligence (EDD), suspicious activity detection, beneficial ownership verification where feasible, and the application of red-flag indicators associated with illicit pharmaceutical activity.

From a regulatory and supervisory perspective, AML/CFT frameworks, Know Your Customer (KYC) requirements, sanctions screening, cross-border payment oversight, and clearer expectations for platform accountability remain central tools, particularly in jurisdictions that permit registration of payment intermediaries and digital platforms.

In parallel, private-sector coordination mechanisms, including information sharing, public-private partnerships, typology development, coordinated disruption of high-risk payment channels, and the strengthening of industry standards, may further improve detection and mitigation of illicit pharmaceutical merchants.

Emerging payment modalities, including cryptocurrency transactions, digital wallets, and other alternative payment channels, continue to introduce potential avenues for regulatory arbitrage and underscore the importance of adaptive monitoring approaches. In this context, risk-based approaches by cryptocurrency exchanges may include enhanced due diligence supported by compliance intelligence providers or analytic tools capable of identifying wallet exposure to known IOP typologies.

In addition, financial institutions and payment providers can play a complementary role in consumer risk awareness by reinforcing warnings regarding high-risk online pharmaceutical purchases, particularly where non-verified vendors or cryptocurrency-based payments are involved, leveraging existing fraud prevention communication channels.

Finally, further consideration may be given to mechanisms that support cross-border financial intelligence sharing specific to pharmaceutical counterfeiting, as well as the development of regulatory frameworks that appropriately incentivize the proactive reporting of suspicious transactions by payment intermediaries, consistent with applicable legal and compliance obligations.

Data availability

Data will be made available on request.

Acknowledgement

This research work was supported by the National Science Foundation in the United States under Award D-ISN-2039779: Collaborative Research: An Interdisciplinary Approach to Understanding, Modeling, and Disrupting Drug and Counterfeit Illicit Supply Chains. The research for this article was made possible by a data sharing agreement and partnership between 3M, Legit Script, and George Mason University (GMU).

References

- [1] Limbu YB, Huhmann BA. Illicit Online Pharmacies: A Scoping Review. *Int J Environ Res Public Health*. 2023;20(9):5748. <https://doi.org/10.3390/ijerph20095748>
- [2] National Association of Boards of Pharmacy (NABP). Rogue Rx Activity Report: Disrupting Illegal Online Pharmacies. Mount Prospect, IL: NABP; 2022. Available from: <https://nabp.pharmacy/wp-content/uploads/2022/10/Rogue-Rx-Activity-Report-Disrupting-Illegal-Online-Pharmacies-2022.pdf>
- [3] Zhao H, Muthupandi S, Kumara S. Managing Illicit Online Pharmacies: Web Analytics and Predictive Models Study. *J Med Internet Res*. 2020;22(8): e17239. <https://doi.org/10.2196/17239>
- [4] Interpol. Record 769 arrests and USD 65 million in illicit pharmaceuticals seized in global bust [Internet]. 2025 Jun 25 [cited 2026 Apr]. Available from: <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2025/Record-769-arrests-and-USD-65-million-in-illicit-pharmaceuticals-seized-in-global-bust>
- [5] Interpol. Online Sale of Fake Medicines and Products Targeted in INTERPOL Operation [Internet]. 2016 Jun 9 [cited 2026 Apr]. Available from: <https://www.interpol.int/en/News-and-Events/News/2016/Online-sale-of-fake-medicines-and-products-targeted-in-INTERPOL-operation>
- [6] Kohler J, Khan A, Bowra A. Bribery and the Global Pharmaceutical Industry: An Exploration of Patterns and Penalties in the Organization for Economic Cooperation and Development Reports. *J Law Med Ethics*. 2026:1-11. doi:10.1017/jme.2026.10237
- [7] Fincham J. Negative Consequences of the Widespread and Inappropriate Easy Access to Purchasing Prescription Medications on the Internet [Internet]. 2021 [cited 2026 Apr]. Available from: <https://www.ahdonline.com/issues/2021/march-2021-vol-14-no-1/3086-negative-consequences-of-the-widespread-and-inappropriate-easy-access-to-purchasing-prescription-medications-on-the-internet>
- [8] ASOP Global. Canadian Internet Pharmacies [Internet]. 2017 Mar 7 [cited 2026 Apr]. Available from: <https://buysaferx.pharmacy/public-awareness-campaigns/drug-importation/faqs/>
- [9] Hertig JB, James SM, Hummel CJ, Rubin MJ. Evaluation of Pharmacists' Awareness of Illegal Online Pharmacies and Perceived Impact on Safe Access to Medicines. *Med Access Point Care*. 2021;5: 23992026211005642. <https://doi.org/10.1177/23992026211005642>
- [10] Schafer A. Canadian Internet pharmacies: Some ethical and economic issues. *Can Pharm J*. 2008;141: 191-196. doi:10.3821/1913-701X (2008)141[191: CIPSEA]2.0.CO;2
- [11] McCoy D, Pitsillidis A, Jordan G, et al. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In: Proceedings of the 21st USENIX Security Symposium; 2012.
- [12] Chainalysis. Crypto Intellectual Property Infringement: Crypto Used in Sales for Illicit Streaming Services and Counterfeit Pharmaceuticals [Internet]. 2024 Mar 29 [cited 2026 Apr]. Available from: <https://www.chainalysis.com/blog/crypto-intellectual-property-infringement-streaming-pharmaceuticals/>
- [13] EUIPO. Intellectual Property Crime Threat Assessment 2019 [Internet]. 2019 [cited 2026 Apr]. Available from: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf
- [14] US Food and Drug Administration. Counterfeit Medicine [Internet]. 2025 Dec 8 [cited 2026 Apr]. Available from: <https://www.fda.gov/drugs/buying-using-medicine-safely/counterfeit-medicine>
- [15] US Treasury. Treasury Sanctions Indian Nationals and Online Pharmacy for Supplying Counterfeit Fentanyl-Laden Pills [Internet]. 2025 Sept 25 [cited 2026 Apr]. Available from: <https://home.treasury.gov/news/press-releases/sb0261>
- [16] OECD and European Union Intellectual Property Office. Trade in Counterfeit Pharmaceutical Products. Illicit Trade. Paris: OECD Publishing;

2020. <https://doi.org/10.1787/a7c7e054-en>
- [17] Tambi S, Biswas G, Kumawat H, Mathur G, Nagaraj A, Shravani G. Counterfeit Medicines Sale on Online Pharmacies in India. *J Res Pharm Pract.* 2014;3(4):145. <https://doi.org/10.4103/2279-042X.145397>
- [18] Eban K. Why Counterfeit Ozempic Is a Global-Growth Industry [Internet]. Vanity Fair. 2024 Jun 4 [cited 2026 Apr]. Available from: <https://www.vanityfair.com/news/story/counterfeit-ozempic-global-growth-industry>
- [19] Dağ P. Counterfeit Cancer Drugs, Human Trafficking, and the Earthquake's Toxic Aftermath: 2023's Best Investigative Stories from Turkey [Internet]. 2023 Dec 18 [cited 2026 Apr]. Available from: <https://gijn.org/stories/2023-best-investigative-stories-turkey/>
- [20] Griffiore KA, Bowra A, Guilcher SJ, Kohler J. Corruption risks in health procurement during the COVID-19 pandemic and anti-corruption, transparency and accountability (ACTA) mechanisms to reduce these risks: a rapid review. *Global Health.* 2023; 19:91. <https://doi.org/10.1186/s12992-023-00994-x>
- [21] World Health Organization. Substandard and Falsified Medical Products [Internet]. 2024 [cited 2026 Apr]. Available from: <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- [22] US Census Bureau. Annual Retail Trade Survey (ARTS) [Internet]. 2023 [cited 2026 Apr]. Available from: <https://www.census.gov/arts>
- [23] Fittler A, Adeniyi L, Katz Z, Bella R. Effect of Infodemic Regarding the Illegal Sale of Medications on the Internet: Evaluation of Demand and Online Availability of Ivermectin during the COVID-19 Pandemic. *Int J Environ Res Public Health.* 2021;18(14):7475. <https://doi.org/10.3390/ijerph18147475>
- [24] Feeney AJ, Goad JA, Flaherty GT. Global Perspective of the Risks of Falsified and Counterfeit Medicines: A Critical Review of the Literature. *Travel Med Infect Dis.* 2024; 61:102758. <https://doi.org/10.1016/j.tmaid.2024.102758>
- [25] Maihold G. Shadow Supply Chains and Criminal Networks. In: Brombacher D, Maihold G, Müller M, Vorrath J, editors. Geopolitics of the Illicit. Baden-Baden: Nomos; 2022. <https://doi.org/10.5771/9783748935940-53>
- [26] We Tranxact. Pharmacy Stripe PayPal Declined UK [Internet]. 2026 Feb 19 [cited 2026 Apr]. Available from: <https://www.wetranxact.co.uk/blog-pharmacy-declined-stripe-paypal-square-uk/>
- [27] Nikos-Rose KM. Digital Payment Platforms Can Easily Be Misused for Drug Dealing, Researchers Suggest [Internet]. UC Davis. 2023 Nov 21 [cited 2026 Apr]. Available from: <https://www.ucdavis.edu/news/digital-payment-platforms-can-easily-be-misused-drug-dealing-researchers-suggest>
- [28] Clark F. Rise in Online Pharmacies Sees Counterfeit Drugs Go Global. *Lancet.* 2015;386(10001):1327-1328. [https://doi.org/10.1016/S0140-6736\(15\)00394-3](https://doi.org/10.1016/S0140-6736(15)00394-3)
- [29] Al-Worafi YM. Counterfeit and Substandard Medications Case Studies. In: Clinical Case Studies on Medication Safety. Amsterdam: Elsevier; 2023. <https://doi.org/10.1016/B978-0-323-98802-5.00006-6>
- [30] Europol. Cryptocurrencies: Tracing the Evolution of Criminal Finances [Internet]. 2021 [cited 2026 Apr]. Available from: <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>
- [31] Chainalysis. The Landscape of Seizable Crypto Assets in 2025 [Internet]. 2025 Oct 9 [cited 2026 Apr]. Available from: <https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/>
- [32] Terrell S. 2026 Canadian Credit Card Report [Internet]. NerdWallet Canada. 2026 Apr 8 [cited 2026 Apr]. Available from: <https://www.nerdwallet.com/ca/p/article/credit-cards/2026-canadian-consumer-credit-card-report>
- [33] Altana. Modernized Border Targeting Using Altana AI [Internet]. 2021 Mar 21 [cited 2026 Apr]. Available from: <https://altana.ai/resources/modernized-border-targeting-using-altana-ai>
- [34] Huang E, Shelley L, Hashemi L. Modelling and Disrupting Counterfeit N95 Respirator Supply Chains. *Adv Eng Informatics.* 2025;64:103084. <https://doi.org/10.1016/j.aei.2024.103084>
- [35] US House Select Committee on China. The CCP's Role in the Fentanyl Crisis [Internet]. 2024 [cited 2026 Apr]. Available from: <https://chinaselectcommittee.house.gov/media/reports/select-committee-investigates-ccps-role-fentanyl-crisis>
- [36] Chainalysis. Can You Track Bitcoin Transactions? [Internet]. 2022 Apr 11 [cited 2026 Apr]. Available from: <http://www.chainalysis.com/blog/is-bitcoin-traceable/>
- [37] Sarker R, Roknuzzaman ASM, Nazmunnahar, Shahriar M, Hossain MJ, Islam MR. The WHO Has Declared the End of Pandemic Phase of COVID-19: Way to Come Back in the Normal Life. *Health Sci Rep.* 2023;6(9): e1544. <https://doi.org/10.1002/hsr2.1544>
- [38] OECD and European Union Intellectual Property Office. From Fakes to Forced Labour: Evidence of Correlation between Illicit Trade in Counterfeits and Labour Exploitation. Illicit Trade. Paris: OECD Publishing; 2026. <https://doi.org/10.1787/540dc43e-en>
- [39] Sahoo M, Singhar SS, Sahoo SN. A Blockchain Based Model to Eliminate Drug Counterfeiting. In: Swain D, Pattnaik PK, Gupta PK, editors. Machine Learning and Information Processing. Vol. 1101. Advances in Intelligent Systems and Computing. Singapore: Springer; 2020. https://doi.org/10.1007/978-981-15-1884-3_20
- [40] Flynn J. 20 PayPal Statistics + Facts [2026]: How Many People Use PayPal? [Internet]. 2022 Dec 7 [cited 2026 Apr]. Available from: <https://www.zippia.com/advice/paypal-statistics/>
- [41] US Food and Drug Administration. Internet Pharmacy Warning Letters [Internet]. 2026 Feb 26 [cited 2026 Apr]. Available from: <https://www.fda.gov/drugs/drug-supply-chain-integrity/internet-pharmacy-warning-letters>
- [42] Galewitz P. Amid Pandemic, FDA Seizes Cheaper Drugs from Canada [Internet]. Kaiser Health News. 2020 Apr 20 [cited 2026 Apr]. Available

from: <https://khn.org/news/amid-pandemic-fda-seizes-cheaper-drugs-from-canada/>

- [43] Shelley L. Dark Commerce: How a New Illicit Economy Is Threatening Our Future. Princeton: Princeton University Press; 2018.
- [44] Lee K.S. Yee, S.M. Zaidi, S.T.R. Patel, R.P. Yang, Q. Al-Worafi, Y.M. Ming, L.C., Combating sale of counterfeit and falsified medicines online: A losing battle. *Front. Pharmacol.* 2017, 8, 268.