United Nations
Interregional Crime and Justice
Research Institute

Project SAVEmed

WP7, Deliverable D7.2
Submission date: M 22

COUNTERFEIT MEDICINES SOLD THROUGH THE INTERNET

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261715

1. OVERVIEW

The present document aims at providing practical indications regarding the risks associated to online sales of counterfeit pharmaceutical products and the modus operandi of counterfeiters who exploit the Internet for their illicit purposes. Moreover, it presents the possible applicability of the indications identified in the analysis on "*Organized crime strategies in the production and sale of counterfeit medicines*" to this area. By highlighting some of the strategies used by counterfeiters and by the networks of criminal organizations which manage such activities we will also address what an anti-counterfeiting technology should take into account in order to better respond to this criminal activity.

The first element to be considered is the role of Internet as an important channel of advertisement and commerce: it may help to better put into context the elements analyzed in this research.

All the EU regulatory agencies' representatives interviewed, which provided relevant information on the illicit trade of counterfeit medicines, confirmed that Internet is becoming the main channel to illegally distribute fake pharmaceutical products.

As a matter of fact the Internet has radically changed the approach towards commerce, drastically modifying also buyers' attitudes towards the purchase of goods in general. Over the last few years the use of fast Internet connections has spread rapidly, giving birth to the phenomenon of online purchases, where a consumer can buy practically every kind of product with a simple click of his/her mouse and receive it directly to his/her door. It is a completely different style of purchasing attitude that rapidly gained the favors of consumers.

Nowadays customers are not only able to buy online almost any kind of product, but they can also easily compare them looking for bargain prices on the basis of their own convenience. With so many different options available, consumers are hardly loyal to a particular supplier and cheap prices are often the primary reason behind their purchase decisions. Buyers usually use this same approach to purchase any type of good, including medicines.

Due to the increasing spread of the e-commerce, online pharmacies started to appear on the Internet with increasing frequency. Even if e-pharmacies often offer pharmaceutical products at cheaper prices than traditional ones, in the specific case of medicines lower costs are not the only driving motive behind online buyers' choices. People suffering from diseases considered as taboos, such as sexual or psychological illnesses, would often rather avoid physical examinations and turn to the Internet for medical advices and treatments. The level of anonymity that is granted by the Internet is an important driving motive pushing some consumers to prefer online purchases. In addition, practical convenience is another good reason. With just a "click", in the comfort of their own home, consumers can buy pharmaceuticals which will be delivered straight to their place. Internet also offers a wider range of products that are not or not yet authorized in some countries. Moreover, the increasing of online sales might be also linked to the increase of a "self-diagnosis" and "self-prescribing" culture.

While on the one side the Internet has created new opportunities for consumers, on the other one it also represents a new powerful instrument that organized criminals have exploited to conduct their illicit businesses. Organized crime has demonstrated a great capacity to exploit every possibility of profit and technological advancement. With the Internet they have found an emerging marketplace that can be exploited in many different ways, taking advantage of the unlimited possibilities offered by the cyberspace. Even the International Narcotics Control Board (INCB) – the United Nations body entrusted with regulating the circulation of drugs subjected to controlled distribution - expressed its concern about the growth of the Internet as a non regulated market[1].

In the recent years the business of online medicines has expanded and become more and more lucrative. This element attracted the interest of organized crime, which could not miss the chance to make profits out of it. Counterfeiters have been exploiting the Internet as an important channel to offer counterfeit medicines both at the wholesale and at the retail level, often creating an independent distribution process which directly targets distributors and final users.

[1] INCB (2010), "Report of the International Narcotics Control Board on the Availability of Internationally Controlled Drugs: Ensuring Adequate Access for Medical and Scientific Purposes".

As far as the distributors are concerned, counterfeiters can penetrate the distribution chain exploiting their constant search for low costs products to maximize their profits. Once they have purchased the pharmaceuticals and marketed them as any other drug coming from an authorized source, it will be almost impossible to trace back the origins of those medicines. Ordinary distribution occurs in conjunction with the supply of drugs through the Internet and may result in the entry of illegal products into the legitimate distribution chain. For instance, within the EU, pharmaceuticals that are purchased from an unauthorized online source by a distributor, due to the single market policy, may be easily spread to any destination within the EU borders. Authorities find it difficult to standardize online market as its operators are usually not located in a single country while, at the same time, restrictions to the business of domestic online pharmacies risk to be considered as an attempt to obstruct the free movement of goods.

For what concerns the retail level, counterfeiters deceive consumers both with low prices and by sending a constant stream of spam messages to their e-mail inboxes. It is clear that the development of new communication technologies and the possibility of exploiting the massive Internet market, has unwillingly favored illegal activities. The result is that the Internet teems with rogue pharmacies selling counterfeit drugs and with fake e-pharmacies that do not sell real goods, but they have the sole purpose to defraud online buyers. These two different typologies of online pharmacies will be better analyzed in this paper. At this stage, it is important to highlight that the lack of a way to identify reliable online suppliers allows the proliferation of shady brokers, resellers and also of the so called «phishers». The latter dedicate themselves to stealing computer identities or money from credit cards used for online purchases. In most cases fake online pharmaceutical shops are driven by organized criminal networks that are responsible for putting citizens' health, together with their personal information and credit card details, at risk.

Spamming plays a very crucial role in the trafficking of counterfeit online medicines. It is an easy, cheap and anonymous way to advertise online goods and it can reach a very large web audience. Spam is thus extensively used by counterfeiters who promote their products by sending unsolicited bulk messages to a very large number of e-mail accounts. The big amount of spam messages sent with the intent of advertising illicit websites also aims at finding potential victims who, in turn, could produce gains for

criminal organizations operating behind the scenes. It is evident that spam messages do not only promote single products but are also often a way to promote an entire illicit website or an illicit chain of websites.

A spam message could consequently promote fake drugs, but also push receivers to visit the illicit websites where counterfeit medicines are sold. In this regards, when creating a rogue e-pharmacy or a fake e-pharmacy, criminals do their best to create an illicit website that resembles at the maximum a licit one, in view of reassuring those unaware buyers who are tempted to perform their purchase in the website. It is not rare that illicit online pharmacies try to mislead consumers by requiring a regular medical prescription in order to allow purchases from their website. This strategy has the sole purpose of reassuring potential buyers on the licit nature of the pharmacy, as eventually the request turns out not to be compulsory and the buyers can easily receive their shipment without any prescription.

Another interesting element regarding the strategies of organized crime selling counterfeit medicines through the Internet is that, in order to maximize their profits, counterfeiters have adapted their offer to the pharmaceutical demand of each geographical area. In developed countries, lifestyle fake drugs have become a scourge for the pharmaceutical market. However, medicines to treat cancer, heart diseases or HIV have not been spared by counterfeiters either. In less developed countries, instead, as priorities and most common diseases are different, counterfeit life saving drugs are mainly sold. Consequently, spam messages received by users in different geographical areas often promote different products, adapted to the specific demand of their area and demonstrating a real selling strategy implemented by criminals. This task is facilitated by the growing expansion of Internet in developing countries. This enlarges the number of potential customers and a growing number of people across the world who may become an easy prey for unscrupulous counterfeiters.

Purchasing medicines through the Internet without taking all the necessary precautions or following spam messages received in email inboxes proves to be extremely dangerous for consumers' health and safety. The involvement of organized crime in this illicit business requires strong counter actions and a participative approach by all the stakeholders concerned. Anti-counterfeiting technologies have a very important role to

play also in the case of online sales of counterfeit medicines, where often the consumer is left alone on his/her purchase choices and needs ways to confirm the authenticity of the purchased products.

2. E-PHARMACIES

Before starting the analysis of illegal websites selling counterfeit medicines, it is important to underline that browsing through the Internet we will surely find a good number of online pharmacies that operate according to the regulations and with transparency. For them, criminals are harsh unscrupulous competitors who advertise fake drugs and put at risk the reputation of all online pharmacies which operate honestly.

In order to support the business of legal online pharmacies some public institutions - such as the Royal Pharmaceutical Society of Great Britain (RPSGM) – as well as private ones – such as the American National Association Boards of Pharmacy (NABP) or the website PharmacyChecker.com – became progressively interested on the issue of online pharmacies, namely of those connected with territorial pharmacies and those operating exclusively through the Internet. Some U.S. and EU institutions have developed an accreditation system for both kinds of e-pharmacies. Those without connection with a territorial pharmacy can take part to a validation programme, go through a series of inspections and eventually conclude their registration. Once their accreditation is complete, pharmacies are listed on the website of the registering institution and are authorized to post the official seal of the institution together with the link of such institution on their own web page. Nevertheless, rough imitations of such seals can often be convincing enough and succeed in deceiving inexperienced online buyers who end up buying fake medicines. A further limitation of these accreditation systems lies in the fact that the institutions named above operate at the national level and, due to the different domestic laws of the various countries, it is extremely difficult for any of them to provide customers with reliable and official information concerning the quality of the pharmaceutical resources available on the Internet.

Rogue and fake e-pharmacies pose a big threat to the business of online legal medicines. In this regard, according to the estimates of the World Health Organization

(WHO) up to 50% of medicines sold through rogue web sites are fakes[2]. Moreover according to the 2010 report of the European Commission's Directorate-General for Taxation and Customs Union (DG TAXUD), the growth of online sales led to a significant increase in seizures of postal parcels, 60% of which contained counterfeit pharmaceutical products.[3]

Such high percentages suggest that fake and rogue e-pharmacies – together with spam messages sent to advertise them – constitute clear signs of the explosion of this illicit business and a good hint towards the involvement of organized criminals that use such instruments for facilitating the trafficking of counterfeit drugs and reaching a higher number of consumers.

It is also important to highlight some recent developments in e-pharmacies marketing activity. Until a few years ago, illegal online pharmacies were using mainly spam on private emails as a way of advertising their products. Spam mainly worked through the profiling of the target. The spammers were often changing their IP address in order to avoid legal controls and spam was the best way to inform their regular and potential clients about their products. Nevertheless, at the present time this practice became less necessary because illegal online pharmacies turned into settled industries based in countries where they result hardly punishable. The merchandising throughout social media has become more widespread and these criminals are more and more frequently big actors within the illicit supply chain.

Another new market sector explored by illegal online pharmacies is the trading of food supplements. Several online companies changed their definition from pharmacies to herbal shops and began to sell food supplements. These products are still not clearly regulated by the legislation at European level and this could well represent a new method through which criminals sell counterfeit drugs under the disguise of a food supplement. In Europe the legal definition of food supplement crosses around the definition of drugs and medicines, often rendering the intervention of the National DRA very difficult or impossible without the support of other national authorities. In the United

[2] Source: WHO news release 2006, full text available here: http://www.who.int/mediacentre/news/releases/2006/pr69/en/

[3] European Commission (DG TAXUD), Report on EU Customs enforcement of IPR – Results at the EU border – 2010, July 2011 (n 17 above)

States the Regulatory Agency FDA has the right of controlling both medicine and food supplements.

The evolution of the counterfeiting system is more frequently involving mid-criminal actors. Several cases throughout Europe have seen the involvement of persons working in gyms or herbal shops: because of the nature of their job, they are very close to potential customers. These actors bought medium quantities of food supplements or common drugs online to be then re-sold to their customers.

All these processes might be increased by the global economic and financial crisis: more people might turn to criminals activities due to the possibility of making profits, and consumers may increasingly searching for products at lower prices, lowering the precautions towards possible risks.

2.1 Rogue and fake e-pharmacies

This paragraph will present an overview of the various typologies of illicit e-pharmacies available on the Internet. In particular it will highlight how legal e-pharmacies have to share a significant portion of the cyberspace with both rogue and fake ones. The latter generally advertised by constant streams of spam messages sent to e-mail accounts all over the world.

Rogue e-pharmacies are those that do not adhere to accepted standards of medicine and/or pharmacy practice, including standards of safety, thus violating regulations, and those that engage in fraudulent and deceptive business practices. Rogue e-pharmacies sell counterfeit pharmaceuticals through ad hoc designed websites which pretend authenticity and often contain features which aim to imitate legitimate ones. Posting logos of various professional and governmental agencies on their websites as well as displaying those of major credit cards or payment mechanisms on the website are very used tactics in order to deceive potential consumers and trying to convince them of their reliability.

Even though over the years consumers' awareness about the presence of such websites has been growing, they largely still seem unable to grasp the risks associated with the

use of counterfeit medicines[4]. In this regard it has to be remarked that the issue of online sales of counterfeit pharmaceuticals does not seem to receive due attention by the media, and certainly the lack of information does not help consumers to make safer choices nor to grasp the real dangers connected to this problem. As a consequence illegal sellers can easily succeed in luring them into buying their products.

Rogue pharmacies are not the only "online subject" trying to deceive consumers, as the Internet teems not only with websites selling dangerously uncontrolled pharmaceuticals that are non-complying with legal standards and regulations, but also with fake e-pharmacies. Through fake e-pharmacies cyber criminals do not really sell medicines, but only use them as baits to defraud online buyers, as in the case of ID theft and credit card cloning. The scheme which often lies behind fake e-pharmacies implies a spider-web composed of numerous websites aiming to attract victims. The goal is to infect the computers of the latter's with a virus - e.g. a Trojan file - in order to steal their valuable data.

Both types of deceptive e-pharmacies - rogue and fake ones - are often efficiently promoted by spam messages, which work even better during times of health crisis, when people go into frenzy over certain types of medicines and when there is a surge of cyber criminals seeking to cash in on the pandemic. For instance such was the case of H1N1 vaccines during the swine flu frenzy. According to the computer security firm Sophos in July 2009 in the UK Internet searches for Tamiflu increased by 1400%[5]. Moreover as announced by the UK's Royal Pharmaceutical Society (RPS) in 2009 the number of Internet scammers[6] offering fake Tamiflu as anti-swine flu drug surpassed those selling counterfeit Viagra[7].

---

[4] As demonstrated by researches carried out by the Italian Ministry of Economic Development and the Italian Medicines Agency (AIFA), such as AIFA, EDQM (2011), *Counterfeit Medical Products and Similar Crimes. Risk Communication.*

[5] "Swine flu fears making millionaires out of Russian hackers", by Graham Cluley, 16 November 2009. article available here: http://nakedsecurity.sophos.com/2009/11/16/swine-flu-fears-making-millionaires-russian-hackers/

[6] The word *scammer* comes from the noun *scam*, which means "a fraudulent business scheme". In slang *scammer* refers to "a person who perpetrates a scam".

[7] "Fake Tamiflu 'out spams Viagra on Web'", by Stephanie Busari, CNN, 03 July 2009. Article available here: http://articles.cnn.com/2009-07-03/health/swine.flu.drugs.warning_1_swine-flu-viagra-h1n1?_s=PM:HEALTH

The following boxes describe the case of a website accused by a French company of selling counterfeit abortion pills and the Italian case of lethal sorbitol. The examples below are just some among the many others involving dubious drugs sold online and circulating through the Internet.

Box 1 – BBC speaks out a websites selling abortion pills

The French firm Exelgyn Laboratoires filed a lawsuit against Women on Web for selling online an abortion pill which was assumed to be composed of mifepristone, but instead turned out to be paracetamol, commonly used as a fever reducer.

In those countries where the practice of abortion is prohibited or strongly limited women who have access to the Internet can buy abortion pills with a simple click on their mouse. As a matter of fact in 2008, according to the news spread by the BBC, the Ru486 abortion pill produced by Exelgyn Laboratoires was available online. Such news caused alarm, as it seemed that no medical assistance was provided to women and because of the risks that those medicines could be fakes.

The British Journal of Obstetrics and Gynaecology carried out a survey on 400 users of the "Women on Web" website, which sells abortion pills "to reduce the number of deaths due to unsafe abortions"[8]. According to the survey the 11% of women who bought such pills had to be hospitalized and go through surgery in order to complete the abortion, whether because the medicines did not work at all or in order to stop the haemorrhage.

Source: "Women using web for abortions" by Jane Dreaper, BBC News, 11 July 2008, available online at: http://news.bbc.co.uk/2/hi/health/7500237.stm

Box 2 – The Italian case of *sorbitol* sold on E-bay

On March 2012 a young woman died in Italy due to a lethal test used to verify food intolerances. Other two women were seriously injured by the same substance. The

[8] Link of the "Women on Web" website: http://www.womenonweb.org/

doctor in charge of administering the test stated to the prosecutor that he was using this kind of test for the first time. Instead of using *glucose*, as usual, he chose to buy online - on the famous auction site e-Bay - this test made up of *sorbitol*, According to the police the real motive would be related to the price: the tests bought online cost about twenty euro less than the ones of pharmaceutical companies. After this case e-Bay stopped all sales of *sorbitol* until the situation would have been clarified. The reasons for the death of the young women still have to be verified.

The Italian pharmaceutical Agency launched the alarm and reacted promptly: out of more than 40,000 on line pharmacies, the legal ones are only a small part, namely the 0.6%, with another 2% of them potentially legal. This means that about 98% of online pharmacies are illegal.

Source: La Repubblica, "*Muore avvelenata da un test antiallergico. Il medico l'aveva comprato su e-Bay*", 25 March 2012

2.2 Deceiving strategies and tools used by criminals running rogue and fake e-pharmacies

Thanks to the Internet, the business of advertisement dramatically evolved and the online advertisements transformed the communication strategies. Basic marketing rules are applied to online advertisement, although the latter proves generally faster and cheaper than traditional advertising campaigns on TV, radios, magazines and billboards. Moreover, by taking advantage of such a tremendous border-free communication tool, the business of advertisement is able to easily reach a huge amount of people all over the world. However the exploitation of the Internet by criminals caused the spread of uncontrolled and unverified pieces of information and products.

As mentioned, spam plays a crucial role as far as the online advertisement and the trafficking of counterfeit medicines via the Internet are concerned. Using electronic messaging systems in order to indiscriminately send unsolicited bulk messages is a cheap and an anonymous way to promote goods on the Internet; it allows targeting and reaching a very large number of people all over the world. Even though companies and

institutions invest lots of money to protect their IT systems against spam, spammers often manage to succeed in breaking the anti-spam systems in place, as it was proven by many episodes occurred and lawsuits settled in the past few years.

Business To Business websites are another good platform potentially exploited by criminals. Some of them sell guns or drugs (cannabis, cocaine, etc…) and they are generally protected by passwords and firewall or need a specific recommendation to grant access.
Also active pharmaceutical ingredients (APIs) can be bought. The acquisition of APIs by criminals normally exploits gaps in the legislation. They are very often bought over the Internet, exploiting the fact that the link between the seller and the customer is hidden. APIs are not covered by the Directive on Falsified Medicines, while they are better covered by the Medicrime Convention.

Internet search engines also unwillingly contribute to keep illegal e-pharmacies in business, as it happened in the case involving one of the most famous Internet search engines, Google, which in 2011 was fined to pay one of the highest penalties ever paid in history by a company in a dispute with the U.S. Government[9]. Google was charged with showing illegal advertisements for fraudulent Canadian pharmacies in the U.S., thus aiding and abetting the problem of illegal pharmacies and making significant profits from it. All this said, it has to be remarked that after Google became aware of the investigations, the company implemented significant compliance measures in order to chase away such illegal e-pharmacies from its website. Indeed it is a fact that the struggle against rogue and fake online pharmacies requires combined efforts at different levels. For instance the adoption of a voluntary code of conduct could demonstrate the commitment of search engines companies in such a fight.

The case of fake abortion pills sold through the Internet presented in Box 1, gives us the possibility to discuss the deceiving strategies put in place by counterfeiters to lure

[9] "Google to pay $500 million to settle illegal ad charges", by Claire Cain Miller, The New York Times, 25 August 2011. Article available here: http://query.nytimes.com/gst/fullpage.html?res=9406EFD91238F936A1575BC0A9679D8B63&scp=2&sq=rogue+pharmacies&st=nyt

potential buyers. Criminals base their selling strategy over the Internet on some basic elements that are, in some cases, connected with the cyberspace itself. Apart from selling their products at lower prices – an element which constitutes an important attractive factor for consumers – Internet sales can also offer a high degree of anonymity to potential buyers and the possibility to easily purchase the products with a simple "click". On the other way around, anonymity is also important for the counterfeiters themselves, who can in many cases be sure that their identity will not be discovered. When consumers purchase their products “behind the screen”, counterfeiters can use a variety of deceiving methods to attract the potential buyers who will never have the possibility to verify the authenticity of what is presented in the fake website selling the products.

Some of these unverifiable elements are surely the logos of genuine online pharmacies or the approval logos of controlling authorities which are often replicated and presented in the fake web-pages by counterfeiters. These elements have the purpose of reassuring potential buyers, as in the case of the request for medical prescriptions. Very often the request of a medical prescription, which is generally indicated by the illicit website as a requisite to allow the online purchase, is only part of the strategy set by counterfeiters in order to falsely reassure their customers. In most cases the online purchase turns out to be permitted even in lack of a regular prescription, as it was shown by a survey conducted by Pfizer on 935 men over 35 years of age. The survey indicated that 50% of the surveyed people purchased online medicines without a prescription and 67% of them bought erectile dysfunction drugs.[10]

The diffusion of the problem is demonstrated by a study of the European Alliance for Access to safe Medicines (EAASM) carried out on a sample of 100 websites selling drugs online. The results showed that 6 times out of 10, medicines bought turned out to be fakes. 62% of medicines bought online ended up being counterfeit or improper, with cases where the information related to the drugs was often not correct and cases where both the packaging and the information leaflet in medicines boxes were deceptive.

[10] “Counterfeit medicines”, The Parliamentary Office of Science and Technology, January 2010 Number 352 – article available online at :
http://www.parliament.uk/business/publications/research/post/publications-by-year/pubs2010/

The following box shows the results of a survey which was conducted in relation to a case of a generic drug that was counterfeited and sold online. It is important to remark that this case only wants to show that every kind of drug can be counterfeit and sold online and it does not want to indicate that generic drugs are more prone to be counterfeited than branded ones. Similar results would have been obtained if the surveyed drug was a branded one.

Box 3 – The alarming results of a survey on the online purchase of generic Prozac

Altroconsumo, the Italian Association for the Protection of Consumers, in collaboration with the *Q-tech Research and study Centre* of the University of Brescia carried out a survey focused on the risks related to the online purchase of a generic drug and in most cases the results turned out to be alarming.

The survey started from the online purchase of a generic antidepressant drug containing *fluoxetine*, the same active ingredient present in Prozac. As it strongly acts on the central nervous system, it requires monitored administration by a medical doctor as well as a prescription for their purchase. Using the search engine Google the researchers were able to identify 98 websites willing to sell the medicine. Out of the total number, 34 of them were immediately rejected as they happened to be duplicate or even "phantom websites" (websites that disappeared from the Internet few days later). The purchase with prepaid card was only possible in 19 cases out of the remaining 64 and was successful - that is to say that the medicine was actually available in the appointed Post Office box - only in 13 cases. Therefore very often not only purchasing online medicines appeared to be like a waste of time and money, but in 31% of cases, after the purchase and the payment occurred, no drug delivery ever took place.

Other contradictions emerged just by checking both the Italian and the English versions of several websites. For instance on Eurodrugstore.eu a medical prescription was only requested on its English version, while it was not on its Italian one. To name another example, Valuepharmaceuticals.com considered a medical prescription as a compulsory element in order to allow the purchase, but eventually to proceed with the purchase it was only sufficient to state that the prescription would be sent afterwards.

However when the 13 successfully purchased packages were finally delivered, researchers carefully analyzed their content. The operation was carried out in a sterile environment in order to avoid any possible contamination or alteration of the products. Chemical and microbiological analysis proved that they were all poor quality or counterfeit drugs, containing toxic ingredients or wrong dosages of the latter or were marked with fake expiration dates. In 8 cases traces of solvents containing possible carcinogenic factors were found.

Source: "Prozac senza ricetta (né benefici). È allarme per le farmacie online", by Laura Bonasera, La Repubblica.it, 24 November 2011. Article available on-line: http://www.repubblica.it/salute/medicina/2011/11/24/news/farmacie_onlie-25476539/?ref=HREC1-5

2.3 The importance of international cooperation against online sales of counterfeit medicines

The risk of purchasing counterfeit products is universally recognized as a growing threat for consumers all over the world. To support the response to the problem, Police, Customs services, Drug Regulatory Authorities and the private sector of various countries all over the world decided to coordinate their action under Operation Pangea.

Such Operation was launched in 2008 as an international day of action, with the aim of tackling the online sale of counterfeit and illicit pharmaceuticals. For the first time illegal online pharmacies were targeted at the international level. In particular the operation targeted three main components used by illegal websites: the Internet Service Provider (ISP), the payment systems and the delivery service. The Operation was co-ordinated by the Permanent Forum on International Pharmaceutical Crime (PFIPC), INTERPOL and the World Health Organisation International Medical Products Anti-Counterfeiting Taskforce (IMPACT).

Along the years the operation gained notable momentum as the number of the participating countries rose from 10 to more than 80 in 2011. The success of the

operations is remarkable not only in terms of participation, but also in terms of findings and results. The four operations carried out between 2008 and 2011 led to increasing numbers of arrests and seizures all around the word. After the success of the first Operation in 2008, in 2009 Operation Pangea II resulted in the shutting down of a number of websites engaged in illegal activities, in the removal of advertisements as well as in the identification of suspects and several arrests. In 2010 Operation Pangea III led to the seizure of more than 2 million pills worth about 6.77 million USD. In 2011 Operation Pangea IV was the largest of its kind, leading to the seizure of 2.4 million illicit and counterfeit pills – including antibiotics, steroids, anti-cancer, anti-depression, anti-epileptic as well as slimming or food supplement pills – originating from 48 countries; the shutting down of 13,500 websites and the inspection of 45,000 packages[11]. Such massive operation involved the efforts of 165 different participating agencies. Its goal was to identify the sources behind illicit pharmaceuticals, to disrupt the online criminal networks and activities connected with the online selling, namely credit card fraud, as well as to raise public awareness of the health risks associated with the purchase of medicines through the Internet.

Due to the almost unlimited possibilities offered by cyberspace, purchasing pharmaceuticals over the Internet is easy while, on the contrary, tracing the various phases within the distribution chain can be a difficult operation. For this reason the cooperation among different Law Enforcement Agencies in different countries becomes essential.

In this perspective, it is worth mentioning the Working Group of Enforcement Officers for counterfeit medicines. It was established for the protection of public health and animal welfare against counterfeit medicines through proper enforcement of regulations concerning the manufacturing and distribution of medicines, termination of illegal activities, and related exchange of information. The first meeting of the HMA WGEO was held in Dublin in 2004, and meetings have been held every six months thereafter under the EU Presidency. Operating at Heads of Medicines Agencies (HMA) level, the WGEO

---

[11] A complete list of data is available here: http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea

is an association of representatives of National Competent Authorities responsible for the manufacturing and distribution of human and animal medicine products in member states of the European Union and the European Economic Area (Iceland, Norway and Lichtenstein), the European Commission, the European Medicines Agency, and Switzerland. WGEO meetings are also attended by representatives of INTERPOL, EUROPOL, and the Pharmaceutical Security Institute. The purpose of the HMA WGEO Meetings is for the enforcement officers to meet every six months to make face-to-face contact with European counterparts to discuss aspects of pharmaceutical crime and particularly counterfeit medicines. It presents a valuable opportunity to share experience, expertise and knowledge and further provides a useful training platform.

Apart from the various operations Pangea, the complexities of the criminal trade created by counterfeiters are also demonstrated by an operation carried out by the U.S. Food and Drug Administration (FDA). Investigators found out that 85% of the pharmaceuticals which were supposed to be coming from online Canadian pharmacies were issued instead from 27 different countries. Spam messages were initially sent from an e-mail address licensed to some person in the Russian Federation; the website server used by counterfeiters was located somewhere in China; the credit card payee phone number was placed in the UK; the card payment was processed in Australia and, lastly, the drugs were sent from the U.S.A.[12]

This case anticipates the topic of spam e-mail messages that will be further analyzed in the following chapter and, once again, underlines how international cooperation proves to be fundamental to effectively dismantle such complex criminal networks operating behind the scenes.

3. SPAM AND THE INVOLVEMENT OF ORGANIZED CRIME

Numerous investigations and seizures all over the world uncovered the strong connection existing among counterfeiting, organized crime and online trade. What we have presented so far allowed us to introduce a series of elements that characterize the

[12] CLARK E. (2008), "Counterfeit Medicines: The Pills That Kill", *Telegraph*, April 5th, available online: http://www.telegraph.co.uk/health/3354135/Counterfeit-medicines-the-pills-that-kill.html

modus operandi of criminals involved in online selling of counterfeit medicines. We have introduced the motivations and the ways in which counterfeiters try to deceive possible consumers visiting illicit online websites. An interesting element on how criminals are able to increase the possibility of success of their deceiving actions by reaching a greater number of potential victims and advertise their products will be analyzed. This is the role of spamming, which can be considered as real advertising actions performed by criminals, against which there is a lack of legislation at the international level. In some countries, as the Netherlands, it is illegal to generate spam inside the national boundaries and every citizen can report an abuse to the authority. In these cases, the legislation could be improved to include also spam coming from external sources. It could be adopted also by other countries as a system to fight fake online pharmacies.

Spamming is more concerned with the offer of counterfeit pharmaceuticals at the retail level, as it targets directly the single consumers. As a result of this criminal advertisement, e-mail inboxes are literally "bombarded" by a constant stream of spam messages offering medicines at cheap prices. The aim is to capture people's attention and lead them to browse the Internet in search of such products to purchase. Very often the spam e-mail contains as well a direct link to the rogue or fake e-pharmacies where customers can be deceived. Spammers are thus contributing a lot to the traffic of counterfeit medicines via the Internet and this is why the following paragraph is dedicated to a more in depth analysis of such phenomenon.

3.1 The role of spam

The term *spam* is used to describe the abuse of electronic messaging systems in order to indiscriminately send unsolicited bulk messages. This definition requires some explanations. More precisely the term *unsolicited* refers to the fact that the message is sent without a verifiable permission granted by the recipient. A message is considered *bulk* when it is sent as part of a larger collection of messages, all of which have an identical content. For instance a job enquiry can be sent in an unsolicited way, but it is still legal. The cases of subscribers' newsletters or customers' communications can be considered bulk, but they have been authorized. Therefore *spam is a problem of consent, rather than content.* In this regard as long as a received message is unsolicited and bulk, it is irrelevant whether its content is an advertisement or a so-called "first

contact letter", such message is still marked as spam. This is a significant element to take into consideration, as attempts to regulate contents of e-mail messages risk to contribute undermining the freedom of speech instead of efficiently fighting the phenomenon of spamming.

The magnitude of the phenomenon is such that, to give some figures, 85% to 90% of e-mails received by most organizations are spam[13]. Spam volumes around the world reach about 250 billion messages a day, that is to say almost 40 spam e-mail messages a day for each woman, man and child in the world.[14]

As it is a cheap and anonymous way to promote products on the Internet, and since it also allows reaching a large number of people all over the world, spamming represents a very powerful advertising instrument.[15] The chance to be able to reach millions of people implies as well the possibility that some of them are actually interested in purchasing such advertised products and therefore it increases criminals' chances to find victims. These are the main reasons why spamming is one of the favorite ways used by organized criminals to advertise their illegal activities and illicit products.

Online trade of counterfeit pharmaceuticals does not escape the rule and medicines are by all means among the most spammed online products. In particular spam messages are very often used to advertise certain types of medicines, such as weight loss pills, or those connected with diseases often considered as taboos, such as erectile dysfunctions or psychiatric/psychological illnesses. In such cases it is particularly easy for spammers to take advantage of consumers' weaknesses. Purchasing such medicines online, with the guarantee of amazing performances and avoiding the shame to go and buy it to a pharmacy, may often seem like an opportunity at least worth trying. Therefore less savvy and less prudent people can easily fall victim of such messages and end up buying dangerous counterfeit drugs.

---

[13] FIRSTBROOK P. (2007), "Benchmarking Anti-spam Effectiveness", *Gartner*, September 18th, *Securing the Network from Spam, Malware and other Threats. A Strategic Overview Featuring Gartner Content*, 3rd issue, Clearswift, available online: http://www.clearswift.com/__data/assets/pdf_file/0020/3674/Clearswift_issue3.pdf

[14] "Spam, a lot", The New York Times, published 13 January 2011. Article available here: http://www.nytimes.com/2011/01/14/opinion/14fri4.html?_r=1&ref=spamelectronicmail

[15] In 2008 researchers calculated that sending a million spam messages only cost 80 USD.

Indeed, as we have seen, very often no prescription is required by rogue and fake e-pharmacies advertised by spamming messages or, when it is required, it only has the purpose to reassure potential buyers of the regularity of the procedures of the websites. The purchase is eventually allowed without a medical prescription. In such cases websites allow the purchase permitting, for instance, that the document will be faxed later.

Given that spam is a common tool among organized criminals, the following are the steps taken to make their operations effective. Once spammers have decided the product they want to illicitly advertise, in our case a medicine or a series of medicines, their next step is to reach an agreement with a website that deals with that type of medicines. In order to find potential buyers, lists containing e-mail addresses to be used as spam recipients are commonly sold between crackers and spammers. Such lists contain million of e-mail addresses, most of which are verified and known to be working. In fact often hackers are charged with targeting websites and retrieving users' e-mail addresses from their databases. For instance if such hackers manage to hack a website offering medicines or healthcare products, users and customers of that website are likely to be interested in products displayed in spam messages and that list is considered very useful.

Maximize their profits by making as many victims as possible fall in their net is part of organized crime strategy. In the case of spam, their aim is of course to try to avoid anti-spam filters in order to be able to reach large numbers of Internet users. That is why often an example of a junk e-mail dealing with medicines could simply just contain an image – for instance a picture describing a pill, a packaging or a bottle of the medicine. The aim is to try to avoid anti-spam filters which, based on a list of "dirty words", should prevent spam messages from being received. In such a case, as the computer software would only detect the image, if the link to which the picture is referred is not blacklisted, the e-mail will pass through the filter. Of course within the past years anti-spam filters have evolved, in the same way spammers have adapted to such evolution though. Nowadays filters are not only designed to protect from messages containing dirty words, but also from those containing certain types of images. This is why spammers have learnt how to realize pictures which do not come out as *jpeg* files or similar thus being able to elude filters.

Once spammers are able to send their messages, the delivery only requires a software designed to send bulk e-mails, for instance *Dark mailer*[16]. It taps into a network of zombie computers and can send up to 500,000 e-mails per hour from a regular cable modem connection. Once spam messages are delivered, spammers only need to wait for their victims to click.

The box below shows evidence of what stated above regarding criminals' ability and strategies to avoid filters. Indeed spammers often manage to succeed breaking anti-spam systems in place, as it was proven by the fake drug scam that involved U.K. college websites.

Box 4 - Fake drug scam hijacks UK college websites

In 2010 a fake drug scam involving unaware U.K. higher education institutions was uncovered. Counterfeiters exploited software flaws in a widely used technology named PHP, utilized to make websites more interactive. Spammers injected a code associated with terms such as Viagra, Cialis and other drugs and each time a person would look for online drugs, universities and colleges' web addresses would pop up. Once online visitors clicked on the link, they would immediately be re-directed to the online fake pharmacy. This is how many organizations using the .ac.uk domain unknowingly pushed customers to websites offering counterfeit pills, thus becoming unaware accomplices of such criminals. According to the researchers, thousands of organizations have fallen victims of such drug spammers.

Source: "Fake drug scam hijack UK college websites", BBC News, published online 5 March 2010 – article available here: http://news.bbc.co.uk/2/hi/technology/8550219.stm

In the past few years several companies settled a series of actions against spammers, attempting to dismantle their illegal activities and thus trying to protect their own

[16] Although there is no official website to download the programme, many websites offer free versions of *Dark mailer,* but most of which often turn out to contain errors and Trojans.

customers. For instance after Viagra was patented, it quickly became one of the most popular drugs as well as one of the most spammed ones. In particular troubles stemming from Viagra spamming reached such an extent that in 2005 a 7-month investigation jointly carried out by Pfizer, the pharmaceutical company which produces the well known Viagra, together with Microsoft, led to a series of actions and lawsuits against physical persons, websites and spam rings linked to illicit online pharmacies in an attempt to dismantle spammers activities connected with the selling of illegal erectile dysfunction drugs. This joint action was an encouraging sign of the determination of the private sector to stop the misuse of the Internet for illegal purposes. Nevertheless there are thousands of other smaller companies dealing with spamming on a daily basis that are unable to dispose of such amount of technological, financial and human resources to get engaged in such a fight.

As spam plays such an important role in the diffusion of fake online pharmaceuticals, the research briefly analyzed in the box below represents an effort to track spam to its source and to collect an overview of the phenomenon.

Box 5 – A pilot study on spam and online medicines

UNICRI, with the support of the International Telecommunications Union (ITU) and in collaboration with an IT security company[17] carried out a pilot study focused on the analysis of spamming with a specific focus on pharmaceuticals. The main aim was to have a better understanding of what lies behind spamming, identifying a possible nexus between spammed recipient addresses and the typology of the received spam messages. The purpose of the research was to prove that a connection actually existed and that spam e-mails were not totally sent on a random basis.

The profiles of the employees of a firm were taken as the target group, their professional e-mails accounts were tracked and their working activities were analyzed.

Thus the analysis of data led to the conclusion that the type of spam messages they received actually changed according to the different profile of the various

[17] Mediaservice is an IT Advisory Security Company based in Turin, Italy.

employees/potential buyers, namely according to the interests, contacts and activities they performed. Specific web searches or the places they visited while on mission could modify the offers and messages they received. Researchers could demonstrate as well that public Wi-Fi networks such as those of hotels or airports were the most exposed to hacking threats. Their insufficiently secured passwords – or total lack of them, – weak firewalls and the anti-virus software they used easily made them an open door for hackers to break in and steal personal data.[18] – Similar outcomes were equally confirmed by a recent research carried out by TrustWave's Spider Labs, according to which hotel networks were hackers' favorite destination in 2009, accounting for 38% of all known security breeches. Moreover, always according to the latter research, it took an average of 156 days before hotels whose networks had been compromised became aware of the fraud, which means hackers had plenty of time to operate.[19] –

Source: UNICRI Programme on Counterfeiting - unpublished material

Different types of Spam

Beyond the daily sending of unsolicited bulk messages to the users, there are other forms of spam - equally effective in the illicit trafficking of counterfeit medicines.

The counterfeiters use to create texts and contents to be published on the web, where reference is made to specific medicines or trademarks. Afterwards:

- These contents can be inserted online into virtual spaces easily accessible by the users, especially places of "social interaction" such as forum or blog. More in general they choose those places that are not protected, so that they can directly and easily reach the potential consumers;
- The counterfeiters can also infringe the rules of copyright, by stealing scientifically important contents from influential websites on the topic. Hence they develop fake blogs through which they are able to mislead and attract the potential consumers;

[18] Spider Labs is an advanced security team within Trustwave focused on forensic, ethical hacking and application security testing. Available online here: https://www.trustwave.com/spiderLabs.php

[19] SMAIL M. (2010), "Hackers Lurking Hotel Networks", 17th March, available online: https://www.infosecisland.com/blogview/3348-Hackers-Lurking-in-Hotel-Networks.html

- Finally, counterfeiters can develop more in-depth actions, by damaging the systems of other websites particularly attended and reliable – such as websites of schools, ministries, hospitals etc. They insert "information packages" on counterfeit medicines, trademarks, and links to their own websites, in order to increase their visibility within the ranking of the most important web engines. This operation allows modifying the algorithms of ranking, making illegal websites more visible and, at the same, time damaging others with a high social utility.

The increasing role of social networks

Although the role of spam has been and is still crucial in the online trade of counterfeit medicines, we have already mentioned how the criminal strategies are progressively changing. While the spam was the main instrument used by criminals until a few years ago, the scenario is now changing. "Social media provide tremendous opportunities for inexpensive word-of-mouth marketing, allowing for the possibility to reach out to more people than ever before"[20]. Instead of using only spam on private emails as a way of advertising the products, at the present time the merchandising throughout social media has become more widespread and the criminals are more and more frequently big actors within the illicit supply chain.

Criminals that are behind the trafficking of counterfeit and illegal medicines are increasingly aware of the extraordinary power of the new social media and social networks over the Internet. Counterfeiters and organized crime are more and more using social networks in order to advertise their products and reach as many consumers as possible. "Links to sites pushing counterfeit wares can […] be found in quantity on social media venues such as social networking sites, blogs and micro-blogs"[21]. On the other side, awareness actions conducted online through social media are not very widespread, especially in relation to the possibility of educating potential consumers on the risks associated with the use of counterfeit medicines and on the importance of avoiding purchasing products online from unverifiable sources.

3.2 The involvement of organized crime in online sales of counterfeit pharmaceuticals

[20] http://www.wordviewediting.com/tag/non-profit-social-media/
[21] https://www.markmonitor.com/download/wp/wp-Fighting_Counterfeit_Sales.pdf

Counterfeiting crimes guarantee the possibility to make large profits and have a very attractive cost-benefit ratio, considering the general weakness of sanctions and punishments in comparison with other crimes. As the main goal of organized criminal groups is to make profits and minimize the risks, they have become very much involved in such illicit business. The following figures concerning the ecstasy trade and the illicit market of the Viagra pills clearly demonstrate the attraction of counterfeit medicines to organized criminals. According to the European Law Enforcement experience it is widely known that a pill of ecstasy costs between 0.20€ and 0.30€ and it is generally sold for an average price of 5€. A Viagra pill costs around 0.15€ and it is sold via an illicit website for around 8€ to 10€. One kilo of counterfeit Viagra pills – 1700 units – costs 255€ and its retail value is from 13,600€ to 17,000€.

Criminal networks often appear to be organized as multinational businesses. Since, unlike legitimate companies, they do not need to comply with any law, pay taxes nor invest in research activities or advertising campaigns, they have an undeniable competitive advantage. Even though they might face losses due to customs seizures or other costs, such as those incurred to bribe officials, they can still make large profits by exploiting well known pharmaceutical brands.

Organized crime is indeed very much involved in the activity of many rogue and fake e-pharmacies all over the Internet. As we have seen above, spam is a powerful advertising tool therefore organized criminals use it in order to expand their market. In this regard organized crime could rather be seen as a veritable illicit enterprise in which spammers hold the role of a sort of an advertising department.

Many spammers, for instance, are located within the Russian Federation; their contribution to the global export of spam is estimated to be such that in 2010 the world spam levels fell also thanks to the shutting down of a payment site for spammers in the country, as it is shown in Box 6.

Box 6 – Spamming drop-off after a Russian website shut down

After Russian police officials announced an investigation on spam flaws, it was noted an evident decline in Russian spamming activities. When the Russian website SpamIt.com abruptly shut down on 27 September 2010, an evident drop-off in spam was noted by various companies monitoring the Internet. Cisco Systems in the United States noted a "sustained drop in global volumes", as stated by one of his senior security analysts, and KasperskyLab, an antivirus company based in Moscow mentioned "a notable drop in mass e-mail in the United States that advertised prescription drugs" from 65% at the beginning of September to about 41% at the end of the month. SpamIt.com was widely known in computer security cycles as one of the larger sponsor of spam in the whole world.

However considering the total amount of spam is approximately around 200 billion per day, although the drop-off of one-fifth was remarkable, the circulating quantity was still far from being a low figure.

Source: "E-mail spam falls after Russian crackdown", by Andrew E. Kramer, The New York Times, 26 October 2010. Article available here: http://www.nytimes.com/2010/10/27/business/27spam.html?scp=7&sq=counterfeit%20pharmaceuticals&st=cse

Criminal operations over the Internet are clearly facilitated by the easy process for registering a domain name and to set up a website in a country, to create a back office in another one and to install an online shop in a third country, especially if one considers that many criminal groups operating at the transnational level already have established alliances and operate in several countries. Once the online shop is operational, it could as well easily direct payments to a fourth country and eventually invest the profits in a tax haven. Moreover very often, in order to further confuse investigators, money is transferred between a chain of bank accounts, creating a smoke-screen which makes investigations more difficult.

Box 7 – Fake pharmacy network tied to organized crime in the Russian Federation

Big amounts of pharmaceutical spam appear to be coming from a fake e-pharmacy, closely linked to organized crime operations in the Russian Federation. According to some researchers of the University of California at San Diego the most actively promoted rogue e-pharmacies via spam would be associated with Rx-promotion.com. The latter would also be associated with ChronoPay, the largest payment processor in the Russian Federation, whose chief executive has been allegedly linked to criminal and illicit businesses, such as that of fake e-pharmacies. According to Brian Krebs, former police investigator, the company bought a license for an Internet service that was used to keep track of ChronoPay black operations, including processing payments for counterfeit prescription drugs sold through hundreds of websites affiliated with the fake pharmacy program Rx-promotion.com. Further investigations led to uncovering other people involved in the fake pharmacy promotion program and were able to identify on the payroll a former Russian police investigator as well.

Source: "Unlicensed pharmacy network tied to Russian mob and corrupt police" by S.Imber, 20 June 2011. Article available here: http://www.safemedicines.org/2011/06/online-pharmacy-network-tied-to-russian-mob-and-corrupt-police-282.html

As underlined by the MHRA, the strategy used by criminal organizations to sell on line counterfeited medicines can be summarized in four main components:

- the domain name;
- the internet provider;
- the payment provider;
- the postal system.

Consumers can be considered as an additional element of the strategy.

In the deceiving strategies put in place by the illicit networks it may be worth to mention the role of the use of postal system. The majority of products purchased on line are delivered in small parcel by postal mail. The small quantities, among the enormous amount of different postal parcels, make their control and identification a very challenging task. As for the different cases and modalities, in several European countries the national authorities investigated cases where packages were mailed to a real address but with a fake recipient, or the contrary, or mailed to P.O. boxes but

without a real address, or mailed, in several deliveries, to a persons in charged of the following distribution.

The postal systems worldwide are regularly deceived by organized crime to perpetrate different kinds of crimes, such as trafficking of counterfeit goods but also drug trafficking, money trafficking and money laundering, marketing frauds etc.
Looking outside Europe, the Canadian Post website reports that for the past few years, unknown organized crime groups have been using the Canadian postal system to distribute Mass Marketing Fraud (MMF) mailings throughout North America. These mailings entered the postal system and tried to legitimize the mailings by including various cover letters, company logos, return addresses, etc. In these cases, like in many others, the fraudsters used legitimate return address and company name in order to make the envelope look more legitimate.

Finally, it is worth mentioning that fake or rogue e-pharmacies managed by organized criminals can reach a high number of people also thanks to the role of small players opening their own small business. It was mentioned how some purchasers over the Internet buy a relatively small quantity of products, sometime keeping part of them for their use and selling the rest to their small circle of customers. In this sense, the distribution is consequently micro-organized, having these players a role of both users and re-suppliers. In this case the consumer is not deceived by the counterfeiters but he/she is most probably aware of what he/she is buying. As it was said, one of the reasons behind the growing of this phenomenon can also be related to the consequences of the global economic crisis on people daily life.

The role of facilitators and the corporate responsibility

As in the case of other serious crimes, such as drug and arms trafficking or pedopornography, the so called “facilitators” should be actively involved in the fight against counterfeiting of medicines. Credit card issuers, money transfers, internet providers, search engines as well as mail services should be involved through tools such as the adoption of voluntary codes of conduct, and awareness raising campaigns. Possible penal liability could be also explored in case the crime is committed thanks to the services provided for by such entities.

The corporate responsibility should be increased among all those actors that are "responsible" at different levels, such as the patient associations, the search engines, the customs, the national and local pharmacy societies, the national governments and international governments as well as the credit card companies and payment providers.

4. FINDINGS

The analysis conducted so far highlighted how the commercialization of counterfeit medicines through the Internet follows its own specific scheme. In fact, it is not always possible to apply those concepts and rules that are typical of the commercialization of products through traditional channels to the case of online sales.

Some specific elements need to be highlighted. The first is surely anonymity, which benefits not only the buyer but especially the seller. Anonymity comes along with the difficulty for potential buyers to verify the authenticity of the offer in the cyberspace. Although several countries have publicly available lists with legal online pharmacies and those authorized to conduct on-line dispensing of medicines, it often remain difficult for consumers to verify the authenticity of the website/pharmacy from which they would like to purchase and they do not have the possibility to verify the authenticity of the product they will receive.

The channel of distribution is also peculiar because if in the case of traditional shipments we will often deal with containers or shipments of great quantities of product, in the case of online sales the shipments involve a limited amount of product sent via regular mail or packaging or by courier. This complicates the detection possibilities by the law enforcers because from a single source it is possible to have numerous small shipments sent all over the world.

The third element to be considered is "access" to the product. In this case the myriad of illicit websites selling counterfeit medicines and the huge amount of spam reaching our inboxes advertising these products render accessibility very easy for potential buyers. Several online counter-campaigns to inform potential consumers on the phenomenon

and its risks have been implemented by national authorities at international level. Some examples are also reported into the “Guidelines. Consumers’ awareness on Internet sales of counterfeit medicines” that UNICRI drafted within the project SAVEmed, such as the online campaigns implemented in Portugal, Spain, UK, Finland, Denmark, Belgium, Italy, Germany, France, Austria among others. The risk information campaigns implemented by national regulatory agencies can be very useful, particularly if their message is effectively tailored to reach target audiences at the different local levels. In many cases consumers are lured by counterfeiters and spammers to visit illegal websites selling counterfeit medicines thus they buy the products without being aware of their real nature. Nonetheless, even in the case in which consumers buying medicines online actually suspect that they are not purchasing an original product, they are totally unaware of the possible risks that counterfeit products can pose to their health.

Another related issue of particular concern is the increasing circulation online of different goods, such as the food herbal products. Since they are not medical products it is impossible to check all of them, also because it is not always clear which is the appropriate authority. Another problem is connected to the difficulties of communicating the risks of buying these kinds of products, since the real effects may vary according to the materials utilized and it is not possible to use the same communication strategies implemented for medical products.

Notwithstanding these peculiarities, some of the suggestions presented in the research of the criminal strategies are applicable also in the case of online sales. In particular: **the need to have a verification tool inside/incorporated by the medicines, the possibility to have a self verification with the packaging, and the possibility to give consumers the chance to check the authenticity of the product they bought**. These three elements would greatly facilitate the performance of controls by National Authorities in the case in which suspicions arise and their implementation would be extremely important to give consumers a series of instruments to check the authenticity of the product they bought. Furthermore **a unique verification number or password** attached to the medicine and to be imperatively communicated to the consumer before the purchase by the online pharmacy could allow for an online verification done by consumers and by law enforcers.

Nevertheless self-verification should not be considered as a definitive solution, as it might help in preventing public health impact, but it does not really help in fighting the involvement of organized crime. However the debate over the reliability of consumers' verification is still open, as self-verification mechanisms would require special tools that once given to the public, could also be available to counterfeiters. Moreover, addressing the issue in ethical terms, the use of self-verification tools may raise some doubts related to the fact that, for instance, such a use would put a very big responsibility on patients and ill people.

On the other way around, the distribution via postal packages creates the need to adapt/modify/render applicable the suggestion aimed at allowing easy checks at all stages of the supply chain. In this case the technology should be flexible and efficient enough to allow also the verification of small postal packages without creating a blockage of the postal distribution system.

The suggestion aimed at creating a link with the intended commercial route does not seem applicable in the case of Internet sales as it is more interesting to prevent the flow of counterfeit medicines via traditional distribution channels and the attempt to infiltrate the legitimate supply chain. Nevertheless cross-sectors and cross-countries cooperation in sharing intelligence information remains a fundamental element to fight the trade of fake drugs throughout internet.

The role of the so called *facilitators*[22] should also be taken into account in the fight against counterfeit medicines. For instance, if a credit card is used to purchase fake medicines, the credit card company should be held liable. In this regard, with due respect to data protection provisions, the creation of a system that could divert money transactions and make them pass through public health authorities for the verification of the money trail could be envisaged, also taking into consideration the problem of data protection.

Another issue that needs to be addressed is the problem of jurisdiction. On one side, criminals are committing these crimes not just in one single country but worldwide. On

[22] The term "facilitators" refers to all those who enable counterfeiters to sell their products, such as fake websites creators, those in charge of payment systems, etc.

the other side, the issue of jurisdiction over the Internet is very controversial and should be regulated since it is easy for organized criminals to create their own heaven in the cyber space.