E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/10/18
ORIGINAL: FRENCH
DATE: SEPTEMBER 8, 2015

Advisory Committee on Enforcement

Tenth Session
Geneva, November 23 to 25, 2015

FRENCH INITIATIVES TO PREVENT AND COMBAT CYBER-COUNTERFEITING

prepared by Stéphanie Leguay, Coordinator of the National Anti-Counterfeiting Committee (CNAC), Directorate of Strategy and International Relations, National Institute of Industrial Property (INPI)[*]

ABSTRACT

We all know, unfortunately, that online counterfeiting is a growing industry. This "scourge" jeopardizes the economic interests of companies in our country and affects practically all business sectors (luxury goods, textiles, cosmetics, toys, spectacle frames, multimedia products…). These products can represent a threat to the health and security of individual consumers in the form of low-quality cosmetics and medicines. On the other hand, counterfeit goods harm the reputation of the trademarks that are copied. The losses caused by the counterfeit market are incalculable.

The National Institute of Industrial Property (INPI), in its capacity as the General Secretariat of the National Anti-Counterfeiting Committee (CNAC), plays a key role in the fight against counterfeiting, alongside other partners. Various types of activities are carried out in order to prevent and combat counterfeiting.

[*] The views expressed in this document are those of the author and are not necessarily those of the Secretariat or Member States of WIPO.

I. PREVENTION

A. AWARENESS-RAISING AMONG CONSUMERS

1. A communication campaign is organized each year in the south of France in order to sensitize the general public. The aim of the last campaign in 2014 was to make consumers more aware of the consequences of online counterfeiting and to support the public authorities during their operations. The campaign was carried out under the aegis of the CNAC in conjunction with the French Customs Authority, INPI and UNIFAB (the Union of Manufacturers for the International Protection of Intellectual Property).

2. Communicating to the general public involved the distribution of more than 100,000 flyers bearing the following message: "Real photos, fake products: Beware of online counterfeiting!"

3. The flyers were designed as a three-fold brochure and targeted the entire family. They contained tips on how to avoid being deceived, an ironic infographic and children's games.

4. The awareness-raising component corresponded to three distinct topics:

- theft of banking information;

- funding of organized crime;

- dangers to consumer safety and the environment.

5. The messages conveyed in the flyer basically consisted of advice, warnings and information illustrated by drawings depicting the consequences of counterfeiting. The aim of the exercise was to make consumers feel that they were accountable for their actions.

6. In order to ensure that the campaign was planned in the best possible way, a number of preliminary actions were carried out simultaneously:

- Shopkeepers, heads of tourist offices and hotel managers in the relevant cities were notified;

- Local operational services were trained and sensitized in order to carry out checks and seizures in conjunction with the police, customs officials and magistrates;

- A national and regional press-relations infrastructure was put into place.

7. Most holidaymakers are aware of the phenomenon. Yet many others still fail to grasp the scope of the problem with regard to consumer products in general. They associate counterfeiting all too readily with the world of luxury goods and the textile industry. It thus seemed sensible to draw attention of summer vacationers towards the counterfeiting of everyday items in order to increasing their insight into the scale and the dangers of the phenomenon as well as the risks involved. For the first time, e-consumers gained awareness and received advice on how to avoid being taken for a ride by all of these fake bargains that they saw on the Internet.

The infographic can be viewed on the following site: www.cnac-contrefacon.fr.

8. The campaign came to an end with highly positive feedback. Year after year, the underlying message of this campaign attracts the attention of increasing numbers of holidaymakers who feel increasingly concerned and better informed with regard to the scale of counterfeiting.

9. Most of the feedback with regard to the message is positive. Sometimes people try to justify their actions or remain in total denial:

- they confess that they have bought counterfeit goods because they wish to follow the latest fashion trends since real fashion items are too expensive;

- "I have already been hoodwinked so I will no longer order online";

- "I don't dare to order online because I fear to be taken for a ride";

- "I didn't think that you could find counterfeit goods online";

- "There are more and more counterfeits in our consumption, in particular online where you don't see the product";

- "What you're doing is really good. We'll take the time to read things in greater detail"; and

- "That's interesting. Maybe we won't get ripped off because we have been warned".

B. IMPLEMENTATION OF VOLUNTARY COOPERATION AGREEMENTS BETWEEN ECONOMIC ACTORS: CHARTERS COMBATTING ONLINE COUNTERFEITING

10. Three voluntary cooperation agreements were signed by various economic actors in order to protect consumers:

- The Charter on the fight against online counterfeiting between intellectual property rights (IPR) holders and e-commerce platforms, opened for signature on December 16, 2009;[1]

- The Charter on the fight against online counterfeiting between IPRholders and online classified advertising platforms, opened for signature on February 7, 2012;[2] and

- The Charter on the fight against online counterfeiting between IPR holders and postal operators, opened for signature on February 7, 2012.[3]

11. These cooperation agreements make it possible to build trust between economic actors who commit themselves to behaving in a balanced and reciprocal manner and to exchange information on a regular basis.

12. The charters include preventive measures (technical detection by the various platforms) and reactive responses (procedures for notification by rights holders).

13. INPI is the authority that follows up on these cooperation agreements. It assesses on a regular basis how these agreements are enforced and, wherever applicable, adapts them.

14. The cooperation between the online sales platforms and trademark holders has led to a significant drop in the number of counterfeit goods being sold on the sites in question.

---

[1] Please also see the presentation of this charter by Pierre Sirinelli in document WIPO/ACE/7/8, available at http://www.wipo.int/meetings/fr/doc_details.jsp?doc_id=186297.

[2] The Charter is available at http://www.economie.gouv.fr/files/Charte_lutte_contrefacon_internet_petitesannonces.pdf.

[3] The Charter is available at http://www.economie.gouv.fr/files/Charte_lutte_contrefacon_internet_titulaires_droits_operateurspostaux.pdf.

15. The charters have made it possible to achieve the following:

- build or create a greater sense of trust between internet platforms and rights holders;

- provide rights holders with the opportunity to submit information in the fight against the sale of counterfeit goods so that personalized proactive detection measures can be implemented (including *a priori*);

- the establishment of mechanisms enabling internet platforms to analyze both the offers and behaviors of sellers;

- notification by rights owners of offers of counterfeit goods to platforms;

- training of platform teams by rights holders with regard to the specificity of the latter's products;

- a regular two-way exchange of information relating to the enforcement of measures included in the Charters;

- this preventive approach has become a standard both in France (Charters of 2009 and 2012) and Europe (a Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet was concluded by the European Union (EU) on May 4, 2011)[4].

16. The approach may be adopted by other countries that are currently looking into the question of new modes of Internet surveillance and are holding consultations with a view to drawing up new regulations on e-commerce. Since July 2014, the French authorities in China (INPI advisers) have been involved in facilitating a direct, matter-of-fact dialogue between Chinese e-commerce platforms and a group of French companies with a view to testing pro-active preventive mechanisms for detecting obvious and recurring counterfeit goods.

II. SUPPRESSION

A. CYBER CUSTOMS

17. The Customs Authority is a highly active member of the CNAC and plays a vital role in combatting online counterfeiting. A Cyber Customs Unit was set up in 2009 to detect Internet customs fraud. To this end, it monitors the people who hide behind pseudonyms on sales websites or in forums, blogs and social media. Its surveillance work can lead to an investigation being carried out by the National Directorate for Customs Investigations and Intelligence (DNRED). The work of the Cyber Customs Unit is essentially limited to websites located in France. If a website is hosted in another country, the investigators' powers are limited to seeking out French buyers involved and international letters rogatory can be issued by an the investigating judge if proceedings are instigated by the prosecution.

---

[4] The English text of Memorandum of Understanding is available at: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf. The Memorandum of Understanding has been described by Jean Bergevin in paragraphs 19 to 27 of document WIPO/ACE/9/20, which is available at http://www.wipo.int/meetings/fr/doc_details.jsp?doc_id=261436. A report from the Commission to the European Parliament and the Council on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (document COM/2013/0209 final) was also published in 2013 and is available at: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A52013DC0209.

18. The Cyber Customs Unit can resort to what is known as the “purchase procedure” in order to establish if illegal trading in counterfeit goods has occurred and to identify the offenders. Introduced into the Customs Code by the Law on the Orientation and Programming for Internal Security of March 14, 2011 (LOPPSI 2), this allows customs officials to purchase a certain number of suspected counterfeit goods in order to verify if an offence has been committed or not.

19. Within this framework, customs officials may use an assumed identity and are logically exempt of any criminal liability. This procedure is effective, but it is sometimes cumbersome for customs officers – with regard to certain offenders – since its application is subject to authorization from the Public Prosecutor. Moreover, Cyber Customs officers are threatened on Internet forums despite using assumed names. Since they do not have the status of cyber-policemen they do not enjoy the same legal protection as intelligence officers (their first names and surnames are indicated in the certified reports).

20. Cyber Customs have to cope with changes in online trading such as the sky-rocketing sales of counterfeit goods on social media (Facebook and Twitter) and the development of drop shopping (goods that are sent directly to the end consumer by the foreign supplier, meaning that the middle-man has no stocks inside France).

21. Cyber Customs officers also have to deal with the growth of the Dark Net. This parallel network can be accessed by means of the free Tor software. The Dark Net is rife with trafficking of all kinds and purchases are generally made using bitcoins (virtual currency which can be converted into real currency). The users think that they are able to enjoy total anonymity, but Cyber Customs have the technical know-how that allows them to locate offenders. The Cyber Customs Unit cooperates with many public actors such as the police and the PHAROS platform (*Plateforme d’harmonisation, d’analyse, de recoupement et d’orientation des signalements*) for reporting illicit content on the Internet.

22. Cyber Customs have also set up partnerships with private operators (online sales sites, rights owners, internet access providers, payment intermediaries). Furthermore, they have secure access to the Internet site of the International Anti-Counterfeiting Coalition (IACC) which handles the reports of rights owners submitted to payment intermediaries (MasterCard, Visa, American Express, PayPal, etc.).

23. Moreover, Cyber Customs are also involved on a regular basis in international control operations related to domain names. “*Operation In Our Sites*” is carried out in conjunction with US Authorities and Europol and consists in identifies fraudulent websites and replaces their welcome pages with a banner that indicates that the afore-mentioned sites have been seized.

24. Unlike their Belgian counterparts, French Cyber Customs officials cannot seize site domains that have been used to commit customs offences. They can, however, refer the matter to the French Network Information Center AFNIC in order to check if certain domain names meet the conditions of accessibility to websites ending in “.fr“. French Cyber Customs can also request implementation of the SYRELI System (a dispute resolution system) which “makes it possible to receive a decision on whether a domain name should be deleted or transferred within a period of two months from the application date”. This is valid only for domain names that are administered by AFNIC (“.fr”, “.re”, “.yt”, “.wf”, “.tf” and “.pm”). The tool is not entirely satisfactory because domain names linked to the committing of an offence are simply “returned to a central repository” from which they can be re-purchased at a later date. Customs officials advocate an extension of the current law. It is suggested, for example, that customs authorities be able to obtain a transfer of ownership of domain names that have hosted illegal content to the State, particularly in the framework of international operations that seek to strengthen control of the Internet.

25. In 2014, French Cyber Customs increased their use of the “cyber purchase“ procedure to combat counterfeiting. By the end of 2014 they had seized approximately 7,000 software items and 1,450 labels counterfeiting the trademark Microsoft on well-known online sales sites. The customs authorities questioned company managers and searched the headquarters and premises shared by the two companies in question.

B. COOPERATION PROJECT WITH ONLINE PAYMENT OPERATORS

26. Finally, a cooperation project with online payment operators is aimed at setting up in France a platform similar to the previously mentioned International Anti-Counterfeiting Coalition (IACC) site.

27. With its Communication “Towards a Renewed Consensus on the Enforcement of Intellectual Property Rights: an EU Action Plan” of July 1, 2014, the European Commission launched an initiative designed to refocus EU IPR enforcement policy towards commercial-scale infringers and the “follow the money approach”. The CNAC seeks to implement a “follow the money” strategy that is aimed at depriving commercial-scale infringers of their revenue streams by drying up the sources of funding for sites specializing in the sale of counterfeit goods. Action is primarily directed towards fostering cooperation between intellectual property rights holders and Internet actors such as e-commerce platforms, remote payment operators and Internet advertising intermediaries.

28. The French Ministry of Culture and Communication has devised a government action plan to combat Internet piracy. A Charter of Commitment engaging advertising professionals in the fight against illicit internet sites was signed on March 23, 2015. Work is currently underway to block the use of online payment methods for sites that infringe copyright. A monitoring committee will soon be set up.

29. The CNAC is also working on a plan to set up an intermediary platform that will bring together all online payment operators and make it easier for companies, particularly small and medium-sized enterprises (SMEs), to ensure that payments are blocked by remote payment operators.

30. With this aim in mind, the CNAC met with members of the Canadian Anti-Fraud Centre (CAFC) in June 2015. In 2011, following complaints from consumers, the CAFC set up a pragmatic cooperation scheme between financial institutions (Bank, Visa, MasterCard etc.), trademark holders, public authorities and consumers.

31. This system allows consumers, who have been victims of counterfeiting, to obtain refunds for the price of counterfeit goods, subject to two conditions:

- proof of counterfeiting must be confirmed by the holder of the right in question and submitted via the CAFC (a sworn authority); and

- the counterfeit goods must not have been accepted.

32. Partnerships have been set up between the CAFC, Visa and Mastercard on the one hand, and the CAFC and Canadian banks on the other.

33. This action is based on already existing policies on fraud involving the use of Visa and Mastercard credit cards, which includes counterfeiting.

34. Consumers who suspect that they might have purchased counterfeit goods and are victims of counterfeit frauds must first contact their banks. Then they are required to send a mail to the CAFC informing it of the name and electronic address of the trader, the address of the Internet site, the name of brand that has been counterfeited, providing a description of the goods and indicating the date and amount of the transaction, the address of the sender and, where applicable, the manner in which the goods were despatched.

36. The CAFC sends this information to the appropriate rights holder, who must then confirm if the goods are counterfeit. Next, the CAFC enters this information into its database. In order to save time, only one confirmation is needed from the rights holder in order to deal with all files relating to the goods in question.

37. The confirmation from the rights holder is then sent to consumers by the CAFC. Consumers subsequently submit the confirmation to their banks in order to receive a refund.

38. The system is quick and efficient because:

- consumers get their money back whenever counterfeiting has been proven;

- counterfeiters forfeit the goods (which are destroyed to prevent resale), and fail to recoup production costs, mailing costs, etc.;

- there is a processing fee of 25 Canadian dollars for chargebacks (certain banks charge more);

- the trader’s bank account is closed by the bank (this takes 1-5 days);

- the trader can be banned from the Visa or MasterCard network;

- the trader is identified as a seller of counterfeit goods by the rights holder;

- the competent authorities in the fight against counterfeiting provide the financial institutions with a notification of investigation and termination, along with a copy of a cease and desist order;

- Canadian financial institutions have a zero-tolerance policy towards sellers of counterfeit goods.

39. Canadian nationals (residing in Canada or abroad) and all foreign citizens who have purchased counterfeit goods from a Canadian company are entitled to contact the CAFC.

40. The CAFC has become a victim of its own success. It has received approximately 9,300 complaints since March 2014. The CAFC team consists of 27 people.

41. Results since 2014 have been positive:

- the activities of 1,600 sellers of counterfeit goods have been identified and stopped;

- approximately 1,000 accounts have been closed;

- 2.7 million Canadian dollars have been refunded to victims, corresponding to an average amount of 288 Canadian dollars per victim.

42. Companies can adopt a pro-active attitude by indicating on their websites that customers should contact their bank quickly.

43. The Nike company has highlighted the advantages of the CAFC's strategy which is free of charge, simple and more efficient than shutting down Internet sites. The information issued by the CAFC is enough to establish whether goods are counterfeit or not. Nike also appreciates the fact that it does not enter into direct contact with consumers (thereby running the risk that a counterfeiter might be able to extract information), working instead in conjunction with a sworn authority.

44. The Canadian system seems *a priori* to be efficient and easy to implement. However, it requires a sworn authority to guarantee reliable information for rights holders and banks.

45. We are examining closely how the Canadian system works and whether it might be introduced in France.

[End of document]