IPRights
MONITORING CENTER
Ukrainian National Office for Intellectual Property and Innovations

Guidelines for responding to misleading payment requests for intellectual property system users

Review of the EUROPOL manual «Procedure manual on handling misleading payment requests for intellectual property system users» supported by EUIPO

IP OFFICE
Ukrainian National Office for Intellectual Property and Innovations

August 2024

Foreword

During the intellectual property registration period, intellectual property rights (IPR) applicants and owners are targeted by fraudulent legal business structures trying to defraud them. Perpetrators offer additional fees or unrequested «services», impersonating competent Intellectual Property (IP) offices or the mimicking of legitimate IP offices.

This document is based on the analysis of the Procedure Manual on Handling Misleading Payment Requests for Intellectual Property System Users, developed by the European Financial and Economic Crime Centre at Europol with the support of the European Union Intellectual Property Office (EUIPO), and does not reflect the official position of UANIPIO.

This review is the result of the activities of the Public Awareness Working Group of the Intellectual Property Rights Infringement Monitoring Center (hereinafter referred to as the IPR Monitoring Center).

The IPR Monitoring Center welcomes any further suggestions or comments on the subject of this Review with the aim of deepening the understanding of trends and challenges in responding to misleading payment requests for intellectual property system users.

List of abbreviations

Abbreviation	Meaning
EUTM	European Trade Mark
EUIPO	European Union Intellectual Property Office
EUROPOL	European Union Agency for Law Enforcement Cooperation
LBS	legal business structures
IPR object	object of intellectual property right

Link to the original manual:

- Procedure manual on handling misleading payment requests for intellectual property system users

Information on misleading invoice and payment request fraud against intellectual property rights (IPR) applicants and owners

First and foremost, EUROPOL advises becoming familiar with the EUTM application and registration process. This knowledge will help assess the validity of communications and documents that may be received from third parties and from the EUIPO during the application and registration period.

The registration process consists of three main stages, which are described below.

Examination period

During the examination period, payment of the basic fee must be made within one month of the filing date, using the EUIPO's specific payment portal. Be aware that the EUIPO will not send any invoices by regular mail or email. On request, the EUIPO can also carry out a search in the EU trade mark database for identical and/or similar marks. Applicants and owners of previously registered trade marks are informed. If no objection is raised, the application for the trade mark will be published online in all EU official languages in the EUIPO daily bulletin. This will be the official start of the opposition period. If nobody files an opposition or third party observation, the trade mark will be registered.

Registration period

When the trademark is registered, the registration and the data of the applicant, including its address, are published online. This is done so that other trade mark owners and the wider public are aware that this particular trade mark is owned by someone. The registration is free of charge and a certificate of registration is issued on the User Area platform.

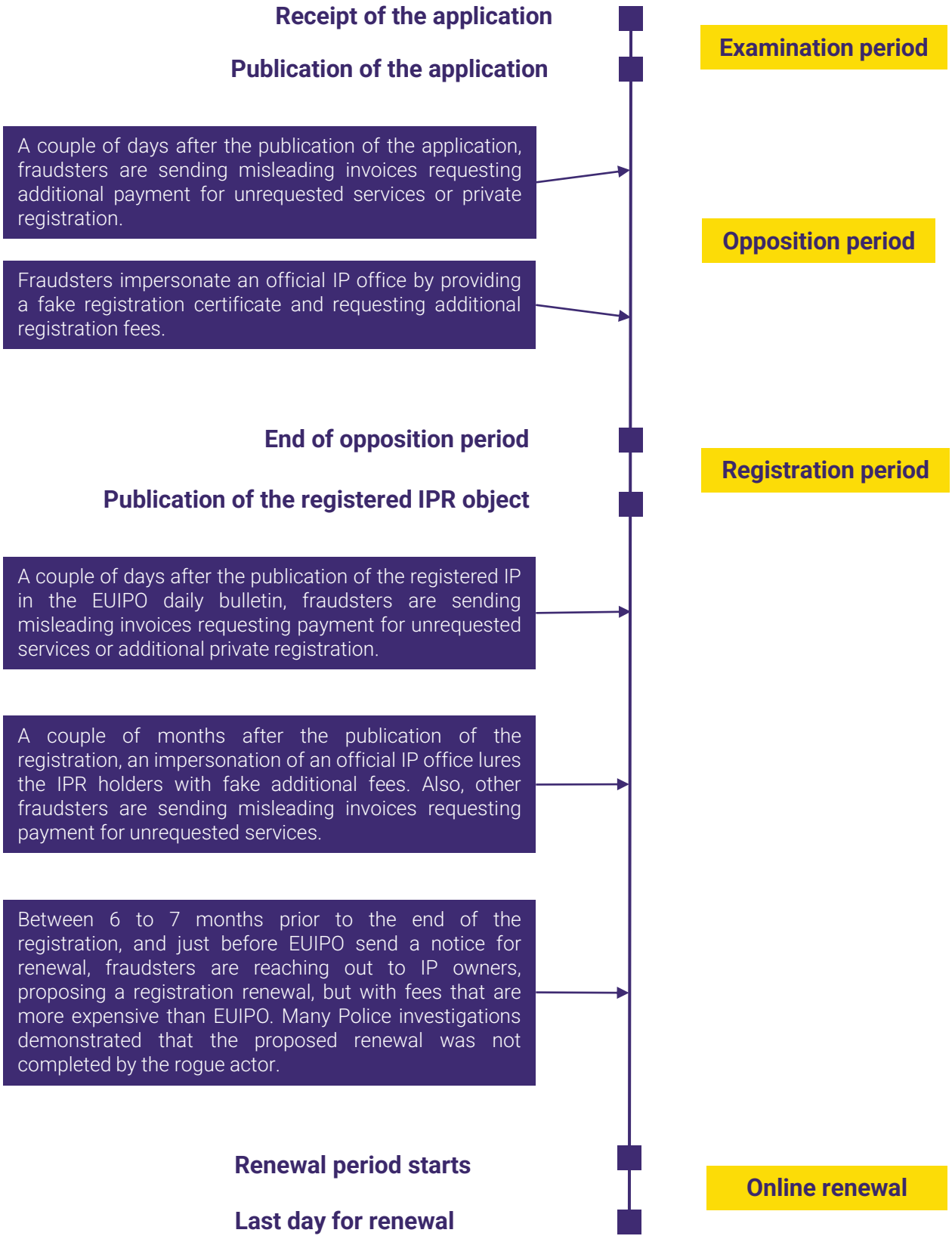
Renewal of registration

A EUTM is valid for 10 years. It can be renewed indefinitely, for 10 years at a time. Six months before the expiry of the registration the EUIPO will inform any person having a registered right in respect of the EUTM that the registration is due for renewal. The EUIPO will always opt to notify by electronic meansthrough an active User Area account, whenever available.

Timeline of the fraud

IPR are at risk from the moment the application is filed, and not only because of the threat posed by misleading invoices. Registering intellectual property is a multiphased and sensitive process during which applicants, particularly direct filers acting without a representative, may experience fear of not being able to protect their IP. The complex nature of the registration process enables fraudulent legal business structures (LBS) to devise new ways of misleading applicant.

Below is a timeline showing the rise in fraud cases linked to each stage of the EUTM registration process.



How to recognise a misleading payment request

It is important to note that the EUIPO never sends invoices or payment requests to users by postal mail or email. The EUIPO electronic application form - eFiling - provides a warning message on this specific risk to users who submit applications through their platform.

Several other national intellectual property offices are also providing warning messages to their applicants, emphasising the need for additional vigilance regarding any correspondence received relating to their IPR.

Fraudsters take advantage of applicants who are still focused on intellectual property registration and fear failure. For example, by analyzing a deceptive invoice from the EUIPO fraud database, the following signs can be identified:

1. **Misleading imitation of an EUIPO trade mark or design.** It is usually placed in the centre of the document to attract attention.
2. **Name and logo of the LBS.** They are placed on the top left, seem familiar but they are different from the genuine national, European or International IP offices.
3. **Sentences highlighted in red.** Sentences placed below or on the same line as the LBS name and logo are intended to shift the IPR owners' suspicious mindset into a frightened one, as the document appears to refer to an important pending payment.
4. **The mandatory VAT number is missing.** The LBS provides no explanation for the VAT exemption or why the amount is EUR 0.
5. **A reminder about the urgency of the payment.** The recipient's attention is drawn to a reminder that the payment is very urgent, typically stating it is due within just eight days. The timespan may be made to appear even shorter, as the date on the envelope can be older than the date on the invoice.
6. **The red color in the messages.** It is used to emphasize the urgency of the payment, which may cause panic among IPR owners who might fear losing their registration.
7. **Mention of the EUIPO.** IPR owners may mistakenly believe that the document was sent on behalf of the EUIPO, forgetting about the top left name and logo of a different LBS.
8. **Bank account.** It differs from the official Spanish bank accounts of the EUIPO.
9. **The fine print.** In light black font, it is stated that LBS provides this as a commercial offer, which is not related to an official IP office, and there is no obligation to pay the requested fees.

How to recognise a misleading email

Nowadays, two types of email are targeting IPR owners:

- misspelling/impersonating emails pretending to be from genuine IP offices;
- misleading emails from an LBS disguising its offer in an invoice.

Criminals rely on the fact that people are too busy to fully read the entire email. At a glance, these emails appear to be legitimate, leading recipients to take their contents seriously and act upon them.

However, there are suspicious elements to watch out for, such as:

- a displayed name that is different to the return address;
- information about a change of bank accounts;
- badly written body copy and message contents;
- infected attachments or suspicious links;
- anguage that creates a sense of urgency.

In case of doubt, how to find valuable information?

First and foremost, users should consult the EUIPO or the respective national office. The EUIPO maintains a searchable common list of scammers on its website, which is dedicated to posting examples of all of the misleading invoice samples reported by users and Anti-Scam Network members. If you have any doubts, you can reach out via: *information@euipo.europa.eu*.

Most of the national intellectual property offices and IPR owners associations are updating their websites with similar information. Further information is available via the links below.

- World Intellectual Property Organization
- European Patent Office
- BENELUX Association for Trade Mark and Design Law
- German Intellectual Property Office
- Irish Intellectual Property Office
- Bulgarian Intellectual Property Office

Reporting misleading invoices and further actions

Identifying a potentially misleading invoice or payment request is the first step within the protection/risk management process. The second - and even more important – step relies on the reporting of the (attempted) fraud either internally or externally.

Internal reporting: report any suspicious payment to your legal department, finance department, or intellectual property representative.

External reporting: report the offence to the relevant authorities (police or the appropriate intellectual property office).

In any case, IPR owners should not destroy the evidence (i.e. envelope and invoice) - it must be included with your report.

How can victims claim their money back?

Recovering money is neither an easy, nor a guaranteed process. This is why we encourage extreme vigilance before making any payments. However, there are at least some means for people to alert the proper authorities and organisations in charge that could be useful.

> *For example,* in some misleading invoices, the IPR applicants/owners will read that they are not allowed to stop the contract and that, even if requested by their bank, the fees won't be refunded. Both statements are in fact misleading. They both violate contract law and would not prevent the IPR applicants/owners from reaching out to their bank to block the transaction, or from reaching out to police authorities.

Both banks and police have ways to liaise with their foreign counterparts rapidly to stop wire transfers and recall money. In their request for blocking the transaction and requesting the money back, IPR owners will have to provide, to their bank counsellor, all evidence gathered demonstrating that the received document was misleading.

Preventive measures - how can applicants protect themselves?

First of all, IPR applicants/owners could implement a procedure to verify the legitimacy of payment requests and check for any irregularities regarding emails, addresses, and phone numbers already recorded in their contact list.

Technical protocols related to domain names and webmail software

For IPR owners/applicants:

Domain Keys Identified Mail (DKIM)

is an internet standard that allows email authentication by detecting forged sender addresses in a spoofed email.

Sender Policy Framework (SPF)

is an email authentication method designed to detect forged sender addresses during the delivery of the email.

The Global Cyber Alliance is providing free tools and information to citizens and legal businesses to upgrade their technical security. For example, ImmuniWeb Phishing Detection Test detects cybersquatting, typosquatting and phishing websites and forged accounts in social networks. This tool helps protect your brand and trademarked material by identifying domains that try to imitate yours as well as domains that contain phishing or malicious content targeting your domain, and more.

Protecting your trade mark is important but taking care of the domain name that could be associated with it is also important.

Trademark Clearinghouse (TMCH)

is a database of validated and registered trade marks, established by ICANN to assist trade mark owners to prevent infringing behaviour in the Domain Name System. The primary purpose of the Trademark Clearinghouse is to maintain a global database of verified trade marks for the Domain Name System and inform its due right owner if someone intends to purchase a domain name using the trademark denomination.

Trademark Registry Exchange (TREx)

is a service developed by the Trademark Clearinghouse, which provides trade mark owners with an additional protection layer for unregistered domain names, matching their labels, across a multitude of top-level domains (TLDs), by restricting the registration of these domain names in the general availability phase.

Domain Protected Mark List (DPML)

allows trade mark owners the ability to block their trademarked names from registration across all of the TLDs supported by a given registry.

Prevention and training on cyber and non-cyber attacks

To improve operational methods and resource management within companies, it is necessary to organise prevention and awareness-raising sessions on various threats. This helps to maintain general knowledge and information on fraud schemes.

We provide below several useful links related to the prevention of intellectual property rights infringements.

- Europol public report on misleading invoice fraud targeting IPR owners
- EUIPO webinar: «Beware of misleading invoices: Act smart against scammers!»
- EUIPO prevention campaign
- Czech IP Office's prevention campaign

Conclusions

Fraudulent activities negatively affect the trust of applicants and intellectual property right holders, thereby undermining the reputation and credibility of intellectual property offices.

The rules outlined in the Manual will help prevent becoming a victim of fraudulent activities in the field of intellectual property and allow for the registration of IP rights with minimal financial risk.

We encourage you to exercise caution with payment requests from national and international offices and to carefully review any notifications before making any financial transfers.