

Misleading payment request fraud targeting intellectual property right owners

2024 Situation Report

Public report



*Funded by the European Union
Intellectual Property Office*



AUTHORS

Europol - European Financial and
Economic Crime Centre (EFECC)

Contents

Key findings	3
Introduction	5
Intellectual property, impersonation, misleading invoice and payment request fraud	5
Aim of the report	6
Background	7
Highlights from the 2021 situation report on misleading invoice fraud targeting owners of intellectual property rights	7
Latest trends – ‘DED scams’, impersonation of national and international IPOs	9
New approach taken by the fraudsters	9
How it started	9
How it developed	10
‘DED scams’ and impersonation of national IP offices	13
Other type of scams against IP system users	18
Same approach, different scenario	18
Misleading invoices	18
Average life of a company	20
Preparation process	21
Criminal findings and links with diverse criminal activities	22
The way forward	24
Warning! From email spoofing to phishing attacks	24
How should recipients of misleading payment requests act	24
Europol and the Anti-Scam Network	26
Recommendations	26
List of abbreviations	28

Key findings

For more than 10 years, intellectual property (IP) system users have been subjected to continuous attacks from scammers from the start of the IP registration process until the end of the protection period. Fraudsters take advantage of intellectual property rights (IPR) owners and applicants' public data¹, to commit this specific cross-border crime. Offering unsolicited and/or fake services or directly requesting an undue additional payment, presented as a normal part of the IPR registration process has developed from a seemingly insignificant, locally-situated crime to a lucrative multimillion crime phenomenon, affecting thousands legal and natural persons in Europe, and even more throughout the rest of the world.

The process of digitalisation and the development of artificial intelligence (AI) tools has also made things easier for fraudsters, who are able to continue exploiting technology to support and develop their own criminal activity. Since the beginning of 2023, in parallel with cases involving postal letter, cases of payment requests sent by email have risen significantly. Even more troubling is that criminal actors impersonating the national or international intellectual property offices (IPO), contact IPR applicants and owners through email, requesting payment of additional fees (from the victims) to complete the process of registration of their intellectual property rights and could also be related to offering unsolicited and/or fake services. More convincing is that scammers attach in certain cases "certificates" to emails that are supposedly-issued by the competent national or international authority. These fraudulent certificates contain official logos, stamps, national/international symbols or QR-codes that redirect the user to existing websites that may be maintained by the perpetrators. Moreover, names and forged signatures of highly ranked officials from the IPO were included as part of the design of these false certificates.

A detailed analysis of the payment requests sent via email revealed that the scammers presumably used both EUIPO's online accessible database and the national IPO's registers as a source of information to identify potential victims. The available sources of information multiply the count of the potential victims. This count would be at least equal to the number of applications that have been filed with the national and international intellectual property offices. In parallel with these new trends, the old-fashioned way of contacting the victims via post remains the most reported and common method for establishing contact.

Digitalisation of the process of drafting and sending misleading payment requests has itself eased the burden on the fraudsters. With the proper knowledge and skills, data related to the victims can be automatically extracted from the EUIPO's online accessible database and again automatically inserted in the emails and the fake certificates addressed to the relevant victims. Nevertheless, scammers may identify from open internet sources any further email addresses which may be used to contact the users. This is even more facilitated with the surge of generative AI systems. The process does not require printers, paper, inks, envelopes, postage stamps, or even physical visits to the post offices or self-service machines, thus saving additional expense and time for the criminals and allowing them to remain anonymous.

¹ In accordance with paragraph 9 of Article 111 of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017, all the data, including personal data, concerning the applicants and the owners of registered intellectual property rights, shall be considered to be of public interest and may be accessed by any third party.

With EUR 1 500² being the average fee requested by fraudsters, the estimated profit generated on a yearly basis is more than EUR 26 million³. This allows them to improve their logistics, innovate, upgrade, evolve and invest in advanced technologies like AI and virtual private networks (VPN), create a network of strawmen recruits, and expand their illegal activity on a worldwide scale. Additionally, aside from the financial damages inflicted on the intellectual property system users, there is also the reputational loss caused to the international and national intellectual property offices to be considered.

Europol actively cooperate with the European Union Intellectual Property Office (EUIPO), the Anti-Scam Network and the law enforcement authorities (LEAs) to observe, gather information, analyse incoming data and to identify new trends, support investigations, generate cooperation and enhance the exchange of operational information between the investigators. The main goal is to prevent and counteract this organised international fraud scheme and raise awareness among the affected parties to reduce their exposure to this threat and the opportunity for them to fall victim to scam.

² Based on the analysis of the contributed information to Europol, there is a reduction in the amount of the average requested fee, compared to 2021.

³ According to EUIPO Statistics for European Union Trade Marks (EUTM) report (2024), available at: <https://www.euipo.europa.eu/en/about-us/the-office/what-we-do/statistics>, the average number of EUTMs published between 2021 and 2023 is 175 000, which represents the number of the potential victims. Based on the analysis of the contributed information to Europol, 1% of targeted victims that reported the scam, actually paid it. Considering this percentage, the suggested number of actual victims may be at least 17 500 victims per year.

Introduction

Intellectual property, impersonation, misleading invoice and payment request fraud

By nature, the procedure of registering IPR is complex, consists of at least three stages⁴ divided in multiple sub-stages. It may take up to several months until the registration is complete.

In accordance with European Union legislation, national or international IPOs are obliged by the law applicable to them to publish data, including addresses of applicants and owners in their publicly accessible register and/or database. There are justifiable reasons for maintaining these registers and keeping them accessible, for the benefit of intellectual property system users. The owners of already registered IPR may oppose the newly applied IP registration if they believe there might be a conflict with their own registrations⁵.

In the IPR registration process, the very instance a person files an application with the competent IPO and their name and address are published is the exact moment at which the prospective IPR right-holder becomes susceptible to fraudsters and their data becomes public and thus available to criminal actors. Fraudsters act swiftly, by enticing potential victims into the misleading invoice and payment request fraud. In this regard, fraudsters exploit customers' insufficient procedural knowledge of the registration process.

The misleading invoice fraud is committed using an invoice or other type of payment request that is not related to a real service or it is related to an unsolicited service and is used to obtain money by deceit⁶. On the other hand, the impersonation fraud is related to false representation of a person that is posing on behalf of someone else⁷, with the sole purpose to deceive the victim and obtain undue financial gain. Scammers combine these two types of fraud with the intention to acquire unrighteous profit from the intellectual property system users.

Between 2020 to 2022, an average number of 24 million⁸ applications were filed per year, including trademarks, industrial designs, patents and utility models. Presumably, this number represents the minimum number of potential victims, on a yearly basis, of this lucrative criminal scheme.

⁴ Examination period, Opposition period, Registration.

⁵ EUIPO, (2024), registration process, available at: <https://euipo.europa.eu/ohimportal/en/web/guest/registration-process>

⁶ Cambridge Dictionary (2024) definition, available at: <https://dictionary.cambridge.org/dictionary/english/false-invoice>

⁷ Britannica (2024) definition, available at: <https://www.britannica.com/topic/impersonation-law>

⁸ WIPO IP Statistics Data Center (2024), available at <https://www3.wipo.int/ipstats/key-search/search-result?type=KEY&key=201>

Aim of the report

The aim of the report is to provide an update on the 2021 strategic report, focusing on the new modus operandi of the scammers: the transition from using letters sent by post to using emails; impersonation of national/international intellectual property offices; and the sources of information used by the criminals.

This report intends to further enhance awareness amongst EU LEA, judicial authorities, and Anti-Scam Network stakeholders⁹ on the topic of acquisition fraud, whilst also describing existing and emerging trends in the EU and worldwide.

⁹ Anti-Scam Network stakeholders are listed in Annex 1 of the Joint Statement on an Expert Cooperation Charter in the Area of the Anti-Scam, available (2024) at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/trade_marks/fees_and_payment/misleading_invoices/Anti-Scam_Network_en.pdf

Background

Highlights from the 2021 situation report on misleading invoice fraud targeting owners of intellectual property rights

Misleading invoice and payment request fraud, targeting IPR owners is a traditional and very lucrative criminal scheme. Scammers use a well-known modus operandi, as described below.

- ▶ To contact their victims, they use several means of communication – post and email.
- ▶ Fraudsters use names that mimic, resemble and can be associated with official competent bodies or directly impersonate them. 80% of the legal business structures involved in the misleading invoice scam, included the words “European”, “Intellectual Property” and/or “Trademark” in combination with register, agency, service, office or institute in its name¹⁰.
- ▶ Several patterns have been detected concerning the logos and symbols used, which include stars, globes and round images. These symbols are associated with unity, alliance and protection. Additionally, the colours that have mainly been used for the logos are blue and yellow – identical to those used by the EUIPO and all European Union institutions.
- ▶ Excluding the cases of impersonation of national/international IPOs, fraudsters send letters that resemble invoices, but are actually offers for unsolicited services. The services they claim to provide are:
 - registration in a private register – a service, which in its nature seems unnecessary, given the fact that both EUIPO and World Intellectual Property Organization (WIPO), as well as the national IPOs, publish the registered IPR and their owners;
 - monitoring service – claiming that they will perform social media and internet monitoring for similarities in the trademark. Based on the information from investigations, no actual service was provided to the IPR owners;
 - renewal services – in most of the cases the offer gives the impression of a proposal for renewal of the trademark in the actual international or national IPO, but in truth this is actually a proposal for renewal in the private register;
 - trademark protection services – given the fact that the EUIPO, WIPO and the national IPOs are the competent authorities to provide protection of the IPR, this service seems unnecessary;
 - unsolicited legal services – offers for support in the process of registration of the IPR.

¹⁰ Based on the analysis of the contributed information to Europol

- ▶ The four main stages during which victims have been targeted by the fraudsters are:
 - targeting the IPR applicants between the publication of the IP application and before the end of the opposition period – in these cases the fraudsters impersonate the genuine IP offices;
 - targeting the IPR owners in a short period (7 to 20 days) just after the publication of the registered IP with the view of luring them to accept unrequested services;
 - targeting the IPR owners several months after the publication of the registered IP with request for payment of additional fees or offering unsolicited services;
 - targeting IPR owners several months or, on some occasions, years before the start of the official renewal process – a more expensive service with questionable effectiveness.
- ▶ Until 2021, most of the letters that contained misleading invoices were sent via post from Germany, Hungary and the Netherlands.
- ▶ In 2021, the average amount of the fraudulent fee was EUR 2 000.
- ▶ Between 1% and 2% of the targeted IPR owners paid the requested fee, which leads to the presumption that the possible annual income for the fraudsters in 2021 may be between EUR 12 and EUR 16 million, considering the amount of IP registered per year.

Latest trends – ‘DED scams’, impersonation of national and international IPOs

New approach taken by the fraudsters

Generating significant profits from criminal activity requires adaptability, innovation, knowledge and organisational skills. In general, criminals that commit different kinds of fraud schemes have found to have these skills and qualities. What is more, they have mastered the art of manipulating their victims. Being agile, inventive, and adaptable to global developments, the criminals evolve at great pace.

The use of emails as part of the misleading invoice and payment request fraud targeting IPR owners or the impersonation of national or international IPOs is not a new phenomenon.

How it started

Since 2019, some fraudulent companies¹¹ have been using emails as part of their communication exchange with the victims. The initial contact begins with a letter sent by post and presented as a contract, which binds the recipient to the fraudulent company. Following the instructions, the victim is asked to complete the application (date, full name and signature) and return it by email or post. Once the document is received, the second stage of the fraud ensues, with the scammers sending the actual invoices via email.

A substantial wave of impersonation attempts of the EUIPO, WIPO, Benelux, Italian, German, Polish and Spanish national IPOs also occurred from 2019 to 2022. The fraudsters requested fees for renewal of the IP protection services or additional fees related to the registration of the IPR sending postal mail letters that often even included the real name of the agency hidden somewhere in the invoice to enhance credibility, and make it seem as if the fraudster is connected to either of the agencies.

¹¹ WPTR (World Patent and Trademark Register), EIPS (European Intellectual Property Services), World Patent & Trademark Agency). All examples of misleading invoices and payment requests on the following pages are extracted from the EUIPO dedicated webpage providing searchable database for misleading invoices and payment requests by IP system users. See European Union Intellectual Property Office, Misleading invoices, <https://www.euipo.europa.eu/en/designs/after-aplying/misleading-invoices>


WPT
World Patent Trademark Register

REGISTRATION OF THE INTERNATIONAL TRADEMARK


AIJ 2024/004

Contract Number: [REDACTED]
Sent Date: 08.05.2024

WPT s.r.o.
Právní zástupce
 Česká Republika
 Tax number: 674591716

Applicant

REGISTRATION DETAILS
Trade-Service(s):


Applicant's Name: [REDACTED]
Published: 28.04.25
International Class: No. Cl.: 11
Mark Type: Trademark, Principal Register

Sign the document within 14 days
 and send it back by e-mail to **office@wpt.eu**
 or by mail to:
WPT s.r.o., Příkop 84/IV, 602 00 Pilsen,
Czech Republic.

Registration Fee	Amount
Registration Fee for 2185103340	1 626,00 EUR
Processing Fee	25,00 EUR
Total Registration Fee	1 651,00 EUR

Registration of the International Trademark:

The trademark applicant has been published in the official journals, which is subject to the Czech Patent and Trademark Office (CPTO). This publishing serves the public of the office. Please note: registration is not a physical act but an administrative one. The trademark is not registered until the registration is published in the official journals. To affirm the right to the trademark, the applicant must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned. The trademark is not registered until the registration is published in the official journals. To affirm the right to the trademark, the applicant must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned. The trademark is not registered until the registration is published in the official journals. To affirm the right to the trademark, the applicant must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned.

Applicant


WPT s.r.o.
Příkop 84/IV, 602 00 Pilsen
 Česká Republika
 IČ: 04888094

WPT s.r.o., Příkop 84/IV, 602 00 Pilsen, Czech Republic. Tax number: 674591716, www.wpt.eu, info@wpt.eu


02107820



Trademark Publication

Contact: info@tps-registrar.com, 800 800 800 800

Reference Number: 18730015

Application Date: 08.03.2024

Application Number: [REDACTED]

Class(es): 42



REPRODUCTION OF TRADEMARK


Publication Fee 995,00 EUR
Additional Fee 0,00 EUR
Total Fee **995,00 EUR**

Publication of the trademark:

The publication of the trademark is the basis of our offer. If you are the proprietor of the trademark, you must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned. The trademark is not registered until the registration is published in the official journals. To affirm the right to the trademark, the applicant must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned. The trademark is not registered until the registration is published in the official journals. To affirm the right to the trademark, the applicant must submit the required documents to the CPTO within the 14-day deadline. If the applicant fails to do so, the trademark will be considered as abandoned.

PLEASE SIGN THE DOCUMENT AND SEND IT BACK.



e-mail: info@tps-registrar.com



Invoice

TPS Service Management AG
 Chatterboxweg 16
 93040 Linsingen
 Germany
 info@tps-registrar.com
 UDI/VAT: CH-013.197.680
 Invoice No. 397.004
 Invoice date: 11/04/2024
 Invoice date corresponds to delivery-service date

08/04/24

Greeting!
 Please find below the invoice for the Trademark publication.

We kindly request that payment is made within 7 days from the date of this invoice. Please refer to the details and payment instructions provided for making the bank transfer.

Pos.	Description	Quantity	Unit price	Total price
1	Trademark publication fee	1	945,00€	945,00€
			VAT 0%	0,00€
			Total Due	945,00€

Payment Instructions:

Account Name:	TPS Service Management AG
IBAN Number:	CH76 0630 0507 2921 4268 5
BIC:	VABECHE22XXX
Bank Name:	Valiant Bank AG
Bank Address:	VALIANT BANK AG, BUNDESPLATZ 4, BERN, Switzerland
Payment title:	Invoice no. 397.004

If you have any further questions, please do not hesitate to contact us.
 info@tps-registrar.com









Best Regards,
 TPS Service Management AG

Per Swiss VAT rules, we charge 0% VAT on services to VAT-registered entities in the EU and non-EU, due to the zero-rated export regulation and reverse-charge mechanism transferring tax liability to the service recipient.

Letter sent in 2019

Letter sent in 2024

Actual Invoice sent by email in 2024

<div data-bbox="284 972 572 1037">  <p>European Union Intellectual Property Office Avenue de l'Europe, 4 05008 Alicante, Spain Phone: +34 965 13 91 00 information@euipo.europa.eu www.euipo.europa.eu</p> </div> <div data-bbox="284 1037 572 1117">  </div> <div data-bbox="284 1117 572 1162"> <p>11.03.2020</p> </div> <div data-bbox="284 1162 572 1220"> <p>DECISION OF THE EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE TO REGISTER A EUROPEAN UNION TRADEMARK BASED ON THE END OF THE OPPOSITION PERIOD</p> </div> <div data-bbox="284 1220 572 1464"> <p>On the day of 05.12.2019 you have applied for a European Union Trademark, per your request to register as the EU Intellectual Property Office, have decided to register your trademark.</p> <p>Trademark name: [REDACTED]</p> <p>Filing date: 05.12.2019</p> <p>Nice Classification: 24.23</p> <p>Owner's name and address: [REDACTED]</p> <p>as the form of a European Union Trademark for an initial period of 10 years starting from the filing date. We hereby kindly request you to pay the registration fee in the amount of 930,00 EUR, calculated according to the EU Regulation No. 2017/1001 on the basis of this decision. The payment shall be made before 25.03.2020 by SEPA bank transfer.</p> <p>Beneficiary: Registration Fees Unit, Avenida de Europa, 4 05008 Alicante</p> <p>IBAN: PL83110422000000000000000000000000</p> <p>Amount: 930,00 EUR</p> <p>Title of bank transfer: pd</p> <p>In case the indicated deadline for the payment is not met, your application for European Union Trademark automatically becomes ineffective and will be designated in the European Union Intellectual Property Office.</p> </div>	<div data-bbox="572 972 987 1037">  <p>Deutsches Patent- und Markenamt</p>  </div> <div data-bbox="572 1037 987 1117"> <p>Hauptabteilung "Information" Deutsches Patent- und Markenamt Zweibühlstraße 12 80331 München</p>  </div> <div data-bbox="572 1162 987 1220"> <p>München, 08.07.2022</p> </div> <div data-bbox="572 1220 987 1464"> <p>Sehr geehrte Damen und Herren,</p> <p>am 07.01.2022 haben Sie mit Ihrer Anmeldung [REDACTED] zum Deutschen Patent- und Markenamt den rechtlichen Schutz der Marke und für sonstige Rechte in der Deutschen Patent- und Markenklasse 12 beantragt.</p> <p>Die Registrierung der Marke sowie die Zahlung in Höhe von 828,00 EUR, die für das Entziehen und Bestehen des rechtlichen Schutzes der Marke und für sonstige Rechte in der Deutschen Patent- und Markenklasse relevant ist, kann spätestens bis zum 18.07.2022 per SEPA-Überweisung auf folgendes Bankkonto erfolgen:</p> <p>Name des Empfängers: Hauptabteilung "Information" IBAN (für Überweisungen aus dem Ausland): PL83110422000000000000000000000000</p> <p>Verwendungszweck: [REDACTED]</p> <p>Mit freundlichen Grüßen Dr. Bernd Löffler Leiter der Hauptabteilung "Information" Deutsches Patent- und Markenamt</p> </div>	<div data-bbox="987 972 1275 1037">  <p>Ministero dello Sviluppo Economico Ufficio Italiano Brevetti e Marchi</p> </div> <div data-bbox="987 1037 1275 1117">  </div> <div data-bbox="987 1117 1275 1162"> <p>Roma, 15 gennaio 2020</p> </div> <div data-bbox="987 1162 1275 1464"> <p>Il giorno 27/11/2019 a mezzo della richiesta marchi [REDACTED] avete presentato all'Ufficio Italiano Brevetti e Marchi la domanda di brevetto con la tutela parallela nel territorio della Repubblica Italiana il marchio d'impresa [REDACTED] della classificazione di Roma 34,3,8.</p> <p>La registrazione di un marchio d'impresa, anche il pagamento dell'ammontare di 600,00 EUR, rilevante per l'attribuzione e la durata della tutela giuridica del marchio d'impresa e per gli altri effetti legali presso l'Ufficio Italiano Brevetti e Marchi, si possono effettuare online o a sua volta il 27/01/2020 a mezzo bonifico SEPA sul conto corrente:</p> <p>Intestato del bonifico SEPA: Destinatario: Dipartimento delle Finanze, Via Mellini, 2, 00187 Roma IBAN: PL83110422000000000000000000000000 Numero bonifico EUR: Causale: [REDACTED]</p>  </div>
<p>EUIPO impersonation attempt 2020</p>	<p>DPMA impersonation attempt 2022</p>	<p>UIBM impersonation attempt 2020</p>

How it developed

The scammers exploited advanced technologies and enhanced their approach towards their victims, by combining impersonation fraud with the possibility of contacting the victims by email. Three main types of impersonation of the national and international IPOs through email were detected – impersonation of the EUIPO, the German Patent and Trademark Office (DPMA) and the Italian Patent and Trademark Office. The list is not exhaustive, as there were also reported attempts of impersonation of the Benelux Office for Intellectual Property (BOIP) and the WIPO¹².

¹² European Union Intellectual Property Office, Misleading invoices, available at: <https://www.euipo.europa.eu/en/designs/after-aplying/misleading-invoices>

In 2021, EUIPO reported a new trend on their official website of fraudsters sending emails purporting to represent the EUIPO. Several scenarios were used by the fraudsters to request undue payment from their victims by impersonating EUIPO.

In the first scenario, the scammers impersonated both EUIPO and the Italian Patent and Trademark Office (UIBM). The fraudsters sent reminder emails with requests for additional fees presented as a requirement for registration in the TMview 'office in Warsaw, Poland'. They relied on the victim believing the legitimacy of the provided information because TMview is maintained by the EUIPO but its headquarters are in Spain and it is not linked to Poland. However, the EU institutions, bodies, offices and agencies are based in different Member States and the European Commission has representations in the Member States, which may lead to confusion and not raise any suspicion in the recipient of the request. Additionally, the funds were requested to be transferred to Polish bank accounts, as opposed to either of the two Spanish bank accounts of the EUIPO¹³, WIPO fees to a Swiss bank account¹⁴, etc., based on the country in which the office is located.

The deadline for the payment is usually set for the day after the receipt of the email, thus intensifying the sense of urgency and impulsiveness. The recipients have limited time to double check the information so they rush to complete the required actions. The concept of intensifying the urgency for payment always runs in parallel with misleading payment requests. Nevertheless, the structure of the request itself raises a red flag for attempted fraud – an impersonal greeting, a time sensitive threat and an unexpected communication. Generally, in formal reminders about a deadline sent via email, the exact date of the deadline is highlighted, in this case, it was not included¹⁵.

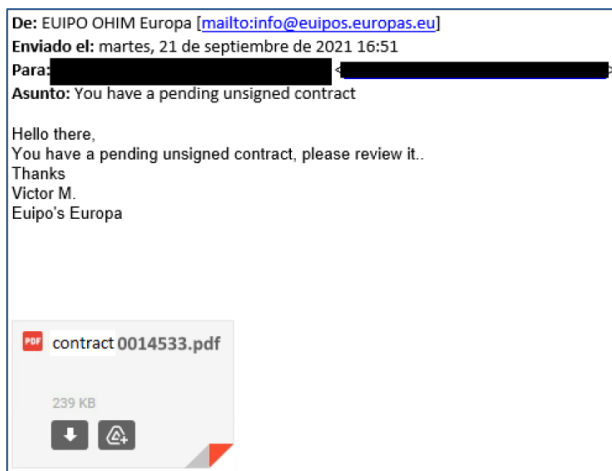
<p>Von: [REDACTED] Gesendet: Montag, 6. September 2021 08:57 An: [REDACTED] > Betreff: Zahlungserinnerung</p> <p>Guten Tag,</p> <p>Diese Informationen beziehen sich auf das Verfahren zur Registrierung der Marke beim EUIPO. Die Veröffentlichungsgebühr in Höhe von EUR 1943,00 ist an das TmView-Büro in Warschau zu entrichten. Bitte tätigen Sie diese Überweisung noch heute, da der Zahlungstermin morgen ist. Bitte senden Sie uns auch die Überweisungsbestätigung schnellstmöglich zu. Dies ist ein neues Gesetz. Unten ist die ursprüngliche Nachricht von TmView.</p> <p>Veröffentlichungsgebühr:</p> <p>Betrag: 1943,00 EUR</p> <p>Begünstigter: TmView Office for Publishing, Krucza 5/11, Warschau, Polen</p> <p>IBAN: PL09160014621852429210000001</p> <p>SWIFT/BIC: PPABPLPKXXX</p> <p>Titel der Banküberweisung:</p> <p>Grüße,</p>	<p>Confidential application reference, if any (please compare with your application): [REDACTED]</p> <p>Your application to the European Union Intellectual Property Office for legal protection of the trademark [REDACTED] is being processed.</p> <p>Pursuant to the EU Regulation No. 2021/1001 of the European Parliament and of the Council of 14 June 2021 on the European Union trademark (text with EEA relevance), every applicant must, in addition to the standard application fee, pay the publishing fee to TmView office in Warsaw.</p> <p>The deadline for the payment related to you application will expire on 07.09.2021. If the indicated deadline won't be met, your application will be disregarded.</p> <p>Publishing fee:</p> <p>Amount: 1943,00 EUR</p> <p>Beneficiary: TmView Office for Publishing, Krucza 5/11, Warsaw, Poland</p> <p>IBAN: PL09160014621852429210000001</p> <p>SWIFT/BIC: PPABPLPKXXX</p> <p>Bank transfer title: [REDACTED]</p> <p>Regards,</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>European Union Intellectual Property Office</p> <p>Avenida de Europa 4</p> <p>03008 Alicante, Spain</p> <p>+34 965 139 100</p>
<p><i>First part of the email</i></p>	<p><i>Second part of the email</i></p>

¹³ EUIPO (2024), Payment methods, Bank transfers, available at: <https://www.euipo.europa.eu/en/trade-marks/before-applying/fees-payments>

¹⁴ World Intellectual Property Office's official webpage (2024), 'How do I pay my Madrid System fees?', 'Bank transfer', available at <https://www.wipo.int/web/paying-for-ip-services/madrid-system-fees>

¹⁵ 'How to Write a Professional Reminder Email' (2024), available at <https://www.grammarly.com/blog/emailing/reminder-email/>

The second scenario of this subtype of scam characterised by its short telegraphic-style content, multiple punctuation and grammar mistakes and informal language does not correspond to the official communication style used by the European Union agencies:



Example of email sent in 2021

Several scamming techniques that developed at a later stage, were used in this early attempt of fraud. The fraudsters spoofed the email¹⁶ address of EUIPO by mimicking the official email and domain name of EUIPO, using typosquatting¹⁷ and also a technique known as 'Addition'¹⁸ – info@euipes.europas.eu – where additional letters are placed in the domain name to resemble one of the official emails of EUIPO – information@euipe.europa.eu.

Additionally, they enclosed a file that required the recipient to take actions, which would lead the fraudsters to their final goal – causing financial damage to the victim to their own benefit.

In 2023, the impersonation attempts continued. Three different approaches have been adopted by the fraudsters – the impersonation of EUIPO, UIBM and DPMA.

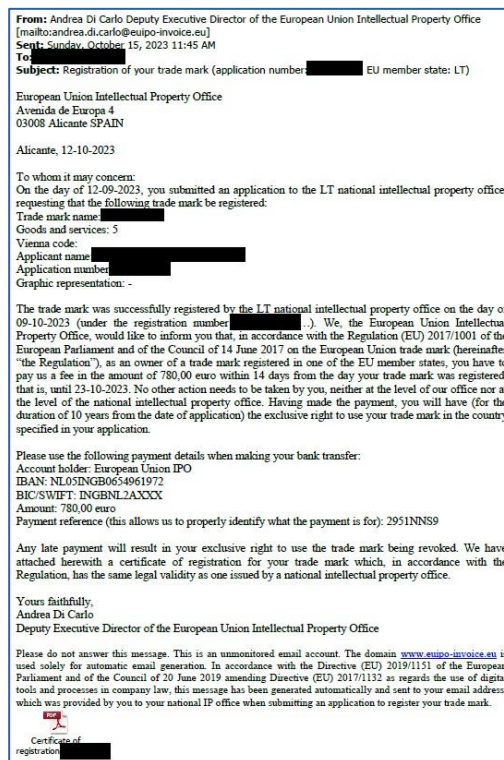
¹⁶ Spoofing: disguising a communication from an unknown source as being from a known, trusted source – definition given in the Internet Organised Crime Threat Assessment (IOCTA) 2023, issued by the European Union Agency for Law Enforcement Cooperation, accessible at <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023>

¹⁷ Typosquatting is a form of cybercrime that involves fraudsters registering domains with deliberately misspelled names of well-known websites with the sole purpose of luring or deceiving visitors for malicious purposes.

¹⁸ An additional letter is placed after the official name in the domain names. Source: 'Focus on Cybersquatting: Monitoring and Analysis' issued by EUIPO on 21st May 2021.

‘DED scams’ and impersonation of national IP offices

In the last quarter of 2023, multiple IP system users from different Member States (MS) were contacted via email sent on behalf of Mr Andrea Di Carlo - the Deputy Executive Director of EUIPO. The email contained an enclosed fake certificate of registration with a forged signature of Mr Di Carlo.



Example of the EUIPO impersonation email sent in 2023

In social-engineering-based frauds, gaining the victim's trust is the first and most essential step which is why the fraudsters used the email spoofing technique to mimic official correspondence with EUIPO. This is a very effective technique used by fraudsters in general, whereby they aim to gain the trust of their victims¹⁹.

In many national or international institutions, it is common practice to send external communications on behalf of senior officials. Taking advantage of this, the fraudsters used the name of Mr Andrea Di Carlo in the email. To ensure that even those not aware of Mr Di Carlo's position in the EUIPO's hierarchy would understand who was contacting them the scammers have manipulated the headers. In the field 'sender', the following text was displayed for the addressee: 'Andrea Di Carlo Deputy Executive Director of the European Union Intellectual Property Office'. Receiving a notification from high-ranking official from EUIPO draws the attention of the recipients especially when they are in a process of registration of intellectual property rights and creates a sense of engagement to fulfil all requests addressed at them.

Additionally, the scammers utilized different variants of the domain names, using the combination between 'euipo' and the words 'mail', 'server', 'notifications', 'invoice', 'registry', etc., divided by hyphen – typosquatting technique known as 'hyphenation'²⁰. The impression of the legitimacy of the email is completed with the usage of the top-level domain (TLD) '.eu' in the sender's domain name. This TLD is mainly associated with

¹⁹ FBI (2024), 'Spoofing and Phishing', accessible at: [Spoofing and Phishing — FBI](#)

²⁰ A hyphen is put between two words in the domain name, to resemble the legitimate one. Source: "Focus on Cybersquatting: Monitoring and Analysis" issued by EUIPO on 21 May 2021.

the EU institutions, agencies and bodies. Nevertheless, there are no restrictions and all EU citizens and organisations established within the EU are allowed to register a domain name using the .eu TLD. Examples of the emails used in this particular fraud are:

- andrea.di.carlo@euipo-invoice.eu
- adnrea.di.carlo@euipo-notifications.eu
- andrea_di_carlo@euipo-server.eu
- andrea_di_carlo@euipo-mail.eu
- andrea_di_carlo@euipo-registry.eu

The main goal of email spoofing is to gain and misuse the victim's trust into requesting certain actions to be taken. In impersonation cases, the aim of the scammers is to persuade the IP system users that they are obliged to pay an additional fee, presented as part of the IPR registration process.

Timing is essential for the development of the fraud. The analysis of the dates on which the emails were sent, compared to the dates on which the applications were filed or the registrations were published in the official registers of the national or international IPO, revealed that the fraudsters contacted their victims between 7 and 14 days following the date of filing the application or its publication.

Analysis of the contacted applicants showed that the registration of the trademark of some of them was refused. That led to the conclusion that the fraudsters use the period in which the IP system users are most vulnerable to contact them – during the opposition period, before the registration of the IP and the official publication. The victim may be eager to accept the requested fees as a normal part of the procedure and pay them, given the fact that the main goal for the applicants at this stage is the successful registration of their IP.

At the beginning of the email, the scammers provide genuine information, related to the recipient – exact date and the place of the submission of the application, the trademark name, goods and services related to the trademark, Vienna code, data related to the applicant, application number and the graphic representation (if available). Most of the applicants are unaware that this data is publicly accessible. Incorporating that genuine information in the email substantiates the legitimacy of the correspondence.

To whom it may concern:
On the day of 28-06-2023, you submitted an application to the BX national intellectual property office, requesting that the following trade mark be registered:
Trade mark name: [REDACTED]
Goods and services: 35
Vienna code: 25.07.01, 25.07.06, 25.07.08, 25.07.25, 27.05.02, 27.05.03, 27.05.07, 27.05.08, 27.05.17, 27.05.24
Applicant name: [REDACTED]
Application number: [REDACTED]
The trade mark was successfully registered by the BX national intellectual property office on the day of 17-10-2023 (under the registration number [REDACTED]).

Extraction of the EUIPO impersonation email

Most of the targeted entities filed their applications with different national IPO from EU MS and not with EUIPO. Random applicants from different countries of origin were contacted at the same time, as three waves of fraudulent emails in October 2023 were detected. It is assessed as unlikely that the fraudsters checked all national IPO's public registers manually or automatically. The most convenient way would be to obtain information from one place, which maintains an up-to-date database, synchronised with the databases of every national IPO, with an efficient and easy-to-use search engine.

The search engine of TMView provides all necessary information and is likely a potential source of information for the scammers. TMview is of great importance for the IP system, supporting its users, saving time and providing access to important relevant information. Maintaining this search engine should be a priority. Nevertheless, the possibility TMView to be exploited by the fraudsters has to be highlighted. This would provide a broader and clearer picture of the fraud scheme, thus assisting the

investigators, the competent national and international authorities and third parties involved in the prevention and counteracting of this fraud scheme.

Midway through the email, recipients are informed of their successful trademark registration in the respective country in which they filed their application. Fraudsters have proven to be manipulative and keen to use different methods to affect the psyche of their victims. They use this approach to predispose their targets, creating the feeling of excitement and satisfaction of completing the main goal, which is to get their IPR registered.

The next step is the direct request for a new payment, which has been presented as part of the official registration process and required in accordance with Regulation (EU) 2017/1001 of the European Parliament and of the Council, followed by a deadline of 14 days. Setting a deadline for fulfilment of a request creates the sense of obligation and urgency. Comparison of the date of the deadline and the date of receipt of the email revealed that the emails were sent on the seventh day before the end of the deadline. This behaviour is intentional and aims to intensify the recipient's anxiety. The victim has been informed that paying the requested fee would be the final requirement and the last action to be done to register the trademark and have it protected for the following 10 years. In general, correspondence that aims to manipulate human emotions to evoke feelings of sympathy, fear, worry or excitement is a clear sign for scam.

We, the European Union Intellectual Property Office, would like to inform you that, in accordance with the Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (hereinafter "the Regulation"), as an owner of a trade mark registered in one of the EU member states, you have to pay us a fee in the amount of 760,00 euro within 14 days from the day your trade mark was registered, that is, until 31-10-2023.
No other action needs to be taken by you, neither at the level of our office nor at the level of the national intellectual property office. Having made the payment, you will have (for the duration of 10 years from the date of application) the exclusive right to use your trade mark in the country specified in your application. Please use the following payment details when making your bank transfer:
Account holder: European Union I.P.O.
IBAN: SK4511000000008216276539
BIC/SWIFT: TATRSKBXXX
Amount: 760,00 euro
Payment reference (this allows us to properly identify what the payment is for): 493N152

Extraction of the EUIPO impersonation email

In the 'DED scams' the fraudsters requested fees between EUR 740 and EUR 780, which is more or less similar to those imposed by EUIPO, being EUR 850 for online registration of one class. Another similarity is the payment reference consists of a seven or eight-character combination of digits and capital letters that resembles the genuine one used by EUIPO.

Analysis on the bank accounts used by the fraudsters in the emails revealed that mainly bank accounts from EU MS (Polish, Slovak, German, Dutch, Italian and Spanish) were mainly used. Using bank accounts originating from EU MS may deceive the recipients and make the request appear more legitimate. However, in the past that scammers have also successfully managed to defraud their victims to transfer undue payments to bank accounts registered outside of the EU, including bank accounts in Georgia, Serbia, Turkey, Egypt, Kazakhstan and even Kenya.

The text of the email is structured in such a way as to persuade the recipient that payment of the fee is mandatory to complete the registration procedure. Right after the payment details, the victim is once again urged to transfer the requested sum, threatened that if the requirements and the deadline are not met registration of the IP will be cancelled.

Any late payment will result in your exclusive right to use the trade mark being revoked. We have attached herewith a certificate of registration for your trade mark which, in accordance with the Regulation, has the same legal validity as one issued by a national intellectual property office.

Extraction of the EUIPO impersonation email

In the last part of the email, the fraudsters included a warning message which can be seen as a counter-measure taken against any attempt by the victim to contact them with additional questions or feedback.

Please do not answer this message. This is an unmonitored email account. The domain www.euipo-notifications.eu is used solely for automatic email generation. In accordance with the Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law, this message has been generated automatically and sent to your email address, which was provided by you to your national IP office when submitting an application to register your trade mark.

Extraction of the EUIPO impersonation email

To solidify the fraud scenario, the fraudsters enclosed fake certificates to the emails that are presented as official documents with legal effect and validity. The genuine certificate issued by EUIPO is rather stylised. However, there are multiple similarities in the design. Most of the targeted entities do not expect to receive certificates from EUIPO, given the fact that they applied for registration in the national IPO and subsequently make payments to the IBAN provided by the fraudsters. Additionally, the fraudsters contact their victims before the registration is complete to ensure that the victim is unaware of the design of the registration certificate.



To be more persuasive the fraudsters included the genuine EUIPO logos several times in the upper part of the fake certificate. Symbols and colours associated with the European Union were also used. A shaded drawing of continental Europe, including MS only, and a circle of 12 yellow stars (a type of pentagram) were used as a background on the certificate. The image in the background resembles the EU flag, which stands for unity, trust, security, solidarity and harmony.

The impersonation of EUIPO goes in parallel with an attempt to impersonate its Deputy Executive Director – Mr Andrea Di Carlo. The fake certificate is supposedly signed by Mr Di Carlo as 'The Executive Director'. This obvious mistake and the information discrepancy within the email are red flags for the attempted scam.

The same pattern with slight changes to the email text and the requested fees can be observed in the impersonation of UIBM and DPMA. The text has been formulated using the same structure of the emails related to the EUIPO impersonation fraud. Higher fees are requested in the UIBM and DPMA impersonation cases, in comparison to the EUIPO case. Functionalities provided by AI may be exploited by the fraudsters, whilst generating different language texts according to the potential victim's country of origin or language used. Including references to either national laws or international

regulations as a basis for the requested amounts further enhances the apparent legitimacy of the actual email.



The UIBM certificate has an extra feature included in its design – a genuine QR code with the EUIPO logo in the centre. The QR code redirects the person to the official TMDN.com webpage. All recipients should be very cautious and vigilant when receiving emails with suspicious attachments as these pose additional risks of phishing attacks.

There are several direct links between the emails and the fake UIBM and DPMA certificates sent by the scammers. The visual similarities and the same pattern used in the design of the certificates are obvious – use of national symbols like coat of arms, official logos, flags, stamps and names of highly ranked officials. At a certain point, the scammers used the same domain name to send fraudulent emails on behalf of UIBM and DPMA – namely <https://www.minister.com>. The use of bank accounts registered in Germany, Poland and the Slovak Republic were also detected in the three cases of impersonation. This may strengthen the assessment that one particular group is involved in this particular subtype of the misleading payment request fraud.

Other type of scams against IP system users

Same approach, different scenario

Apart from the impersonation of national and international IPOs, another cluster of fake companies has been actively contacting IPR applicants or owners via email offering fake legal services and promoting trademark protection and monitoring services. They use different names that sound legitimate and resemble the official competent organisations:

- IPR Protection
- EuroProtect Trademark Solutions
- EU Brand Protection
- Europe IP Protection
- EuroMark Protection Services, etc.

All of the above-mentioned fraudulent companies use the same *modus operandi* to contact their victims, by sending emails, providing the same fake information and applying the same fraudulent IPR registration approach. The scammers request additional fees to solve the problem that an alleged third party intends to apply for the registration of the same mark. They set a deadline, with the emails being translated into different languages according to the origin of the recipient. Since the emails reported were in Danish, Dutch, English, German and Norwegian, it is highly likely that the scammers exploited different online tools to generate the text in different languages. To develop and support their scamming activity, they register websites with different domain names, but using the same content – www.eufts.com, www.eubrandprotection.com, www.euipp.com, www.eumps.net. This cluster of companies has been actively contacting victims since 2022.

Involving the victim into a non-existing problem, whilst providing the solution with a payment option is a typical *modus operandi* for different types of frauds – including shock call frauds, CEO frauds and romance scams. The fraudster's main aim is to gain undue profit and cause financial loss to their victims.

Misleading invoices

The conventional method of sending postal mail letters with misleading invoices offering unsolicited and fake services such as registration in a private register, trademark protection and monitoring services, trademark renewal or legal services remains the main method for contacting the IPR applicants and owners and the most reported one by EUIPO's customers.

Since 2022, more than 2 000 misleading invoices and misleading payment requests have been reported in the Customer Department of EUIPO. An in-depth analysis has been carried-out to obtain additional information on the emerging trends, new *modus operandi* and new approaches taken by the scammers.

In comparison with the fraudulent companies active in 2020-2021 there are minor differences in the used names and the logos. In general, the names used by the companies use the following construction and combination of the adjectives 'European',

‘World’ or ‘International’ + the phrase ‘Intellectual Property’ and the nouns ‘protection’, ‘office’, ‘agency’, ‘services’, ‘trademark’, ‘directory’, ‘organization’. Using this construction, they create multiple different combinations. EUIPO keeps track of and provides an up-to-date list of legal business structures, suspected to be active in the misleading invoice scam through their dedicated website²¹. Some of the active suspected entities between 2022 and 2024 are as follows:

- EIPO – European Intellectual Property Office
- EIPS – European Intellectual Property Services
- EPTA – European Patent and Trademark Agency
- EPTP – European Patent & Trademark Protection
- EUIPA – European Intellectual Property Agency
- EUOIP – European Office Intellectual Property
- IPATD – International Patent and Trademark Directory
- IPRO – International Patent Research Office
- IPTO – Intellectual Property Trademark Organization
- IPWU – Intellectual Property World Union
- ITPR – International Trademarks Publication Register
- TPS – Service Management
- TRS – Register
- WOIP – World Organization Intellectual Property
- WTPR – World Trademark & Patent Register

Globes, stripes and stars continue to be used as part of the logos of the fraudulent companies, as symbols of unity, alliance and dynamism. Some of the companies that offer trademark protection services used the symbol of the shield, associated with safeguarding, security and power to provide safety. The majority of the logos used by the fraudsters include the blue and the yellow colours. These colours resemble the colours and symbols of the European Union and its institutions. The scammers strive to create a fake image that their companies are trustworthy international organisations that provide real services and act efficiently at a cross-border level.



Logos used by different companies suspected to be involved in the misleading invoice and payment request fraud

²¹ European Union Intellectual Property Office, Misleading Invoices, <https://euipo.europa.eu/ohimportal/en/misleading-invoices>

The link between different companies is obvious. They can be divided in several clusters based on similar elements such as common invoice template, exactly the same website content, similar name and logo and IBANs with same country of origin (Egypt, Kazakhstan, Poland, Slovak Republic). It is assessed that several criminal networks are constantly active in the scheme and just rebrand the name of the fraudulent companies. This may be an act of precaution taken by the fraudsters, or alternatively they are forced to adopt this approach, in order to be active within a shorter period, whilst also being more operative and effective. The reason may also be related to ongoing investigations into the companies or actions taken by banking institutions based on suspicious transaction reports (STR) or analysis. The criminals developing this organised international criminal scheme appear to be well informed and experienced. Most certainly, they are aware of the challenges and time-consuming procedures related to the international investigations and cooperation. The scammers often include a small, barely visible text at the end of the misleading invoices. They seem convincing to the receiver as it appears to be a confirmation that their application will be protected.

Dear Madam/Sir,

Offer

your Community Trade Mark application data has been submitted to the European Union Intellectual Property Office to be taken under legal protection on the territory of the Member States of the European Union. The publication of your Community Trade Mark application, which above lists the reproduction of the Community Trade Mark, Application Filing Number, Application Filing Date and Date of Publication are basis of our offer to register in our private database website. Please note, that publication is not affiliate with the official Community Trade Mark edition and is not a publication by a government entity. Your payment confirms this offer herein. Entity is valid for one year. The contract period starts when your payment has been received. This offer is not an invoice. You are under no obligation to pay the amount unless you accept this offer. We also refer to our terms and conditions under www.ipto-service.com. The contract will automatically be renewed, if you not terminate the contract three month prior to the Contract expiration. European Office: Avenue Louise 65/11, 1050 Bruxelles, Belgium

Text included by the fraudsters in the misleading invoices

Average life of a company

Based on the analysis of the information shared with Europol, the average lifespan of a fraudulent company is 12 months. At a certain moment, at the end of Q1 2023, there were at least eight companies actively disseminating misleading invoices synchronously. Mass mail attacks against IP system users may result in a total loss of trust in the official national and international authorities with competence in the area of IPR protection and responsible for IPR registration procedures. Additionally, there are companies assessed to have been actively engaged in this fraud scheme since the beginning of 2021.



Timeline of the average life of fraudulent company

Preparation process

The process of committing this organised international crime requires strict organisation and well-developed logistics, regardless of the method of contacting the victims – via postal mail or email.

The first requirement that plays a crucial and fundamental part in both cases is the bank account. Since 2022, more than 114 different bank accounts, held at 48 banks, have been used in misleading invoice and payment request frauds. Additionally, some of the payments were requested via cheque. The statistics indicate that Germany, Poland and Slovak Republic are the countries in which most of the bank accounts were registered within the EU. The list is not exhaustive – as some of the bank accounts were registered in Bulgaria, Czech Republic, Greece, Italy, Lithuania, Netherlands and Spain. Egypt, Kazakhstan, Serbia and Switzerland are the leading places for bank accounts held outside of the EU.

To comply with and facilitate their customers' requirements, most banking institutions have adopted methods that permit clients to open a bank account virtually, without needing to be physically present at the bank. Although it is very convenient for regular customers, this functionality has been exploited and misused by criminals. In most cases, the 'Know Your Client' (KYC) procedure adopted by banks requires a photo or short video record of the face of the customer, a photo of ID document issued by the government (ID card, driver's licence or passport) and 'proof of address'²². Scammers use different options to bypass these requirements:

- Forgery of the requested documents and photos²³.
- Use of straw man company directors²⁴.
- Committing predicate crimes with the sole purpose of assisting and facilitating the main criminal activity – for example, phishing attacks aimed at stealing someone's personal details with the view of exploiting them for bank accounts registration.

A comparison between the cost of using the post and sending emails to commit these crimes naturally comes out in favour of emails being cheaper.

The dissemination of misleading invoices by post requires additional expenses – postage stamps, envelopes, paper, printing machines and inks. Most of the reported misleading invoices were sent by post from Germany. Since 1 January 2022 the price of sending a standard letter in Germany is EUR 0.85²⁵. To complete the scam, fraudsters have to rely on multiple stakeholders – hosting companies, mailing and printing legal business structures that require additional investment. Since January 2022, more than 2 000 misleading invoices and payment requests have been reported to the EUIPO Customer Department. These numbers represent only the minimum number of victims targeted in general. Considering the investment in postal letters and the cost of printing, the associated expenses is assessed to be more than several thousand euro.

For comparison, the estimated average price²⁶ for registering top-level domain for one year is USD 9 – the price of TLD '.com' is USD 11, '.org' is USD 8, '.eu' is USD 5 and '.net'

²² Proof of address – a document that verifies where a person lives – utility bill, bank statement, rental agreement, official government correspondence. It must include the full name of the person and their residential address.

²³ Websites offering A.I. generated IDs and packages with all necessary documents for passing the KYC check are available on the internet: example (accessed in 2024): [Passport PSD Template — buy editable passport photoshop template | Passport Cloud \(passport-cloud.net\)](#). Some of them were taken down by LEAs: archive webshot of website taken down in the beginning of 2024: [Document Templates Generator - Create Custom Documents Online \(archive.org\)](#)

²⁴ A person to whom title to property or a business interest is transferred for the sole purpose of concealing the true owner and/or business machinations of the parties. Source: <https://www.dictionary.law.com>

²⁵ https://www.shop.deutschepost.de/en/b/brief_postkarte.html

²⁶ Average price taken from hosting and domain services provider, used by the fraudsters to register fraudulent domain names. Source: <https://www.namesilo.com/pricing>

is USD 13²⁷. The price of the WHOIS privacy service²⁸ is included in some of the offers, and if it is not, this is an additional expense. The scammers use VPN services to shield their communications and complicate the tracking process. Apart from the free VPN offers, the average price of the paid service is USD 5 per year²⁹. The registration of domain names and purchase of VPNs can be paid for in various ways – e.g. credit card, PayPal, bank transfers, crypto currencies (BTC – Bitcoin).

The scammers aim to make the criminal scheme more efficient and less expensive. A comparison of the cost of the traditional approach using the post and the email method reveals that email correspondence is more convenient and cheaper. Additionally, it provides better anonymisation for the scammers. The equipment needed to commit the fraud is a computer and internet connection. The shift from post to electronic mail follows the worldwide trends of digitalisation.

Criminal findings and links with diverse criminal activities

There are currently several ongoing investigations across Europe into companies actively disseminating misleading invoices and payment requests.

As a result of the active investigations by competent LEAs, the analysis of the incoming data and the enrichment of that data performed against Europol's database, the following findings can be shared:

- ▶ There is direct evidence that some of the active scammers changed their approach from post to email. This is a clear sign of the evolution and the development of the ongoing scams.
- ▶ Personal data of refugees and migrants have been used for registration of bank accounts in EU MS. Once the bank account is registered, the criminal actors gain control and perform withdrawals on their own. To obtain refugee status, the persons have to undergo a procedure that requires them to register at a specific address in an EU MS. In certain cases, one address is used for the registration of tens and even hundreds of individuals. In practice, none of the registered persons could be found at the address. This creates difficulties for investigators to locate and interview the holders of the bank accounts. When they manage to speak to them, the account holders are not aware of the malicious purposes for which their accounts have been used.
- ▶ Use of 'money mules' – persons with criminal records, a low income or in vulnerable situations, or others who may not suspect criminal activity, are hired to seemingly legitimate jobs that promise quick and legal gains. In most cases these jobs are advertised on the internet or via direct messages through instant messaging mobile applications. Money mules receive money from third parties into their bank accounts and either transfer it onward to a third

²⁷ Most used TLD by the scammers to register websites as part of the process of creating a fake image of their fraudulent companies.

²⁸ The domain name registrars replace the user's personal data in the WHOIS with information of a forwarding service. The aim of this service is to hide the data of the user.

²⁹ Price comparison on the top VPN providers. Source: <https://www.security.org/vpn/cost/#how-much>

party, withdraw the cash or hand it over to someone else for a commission.

Money mules are involved in the criminal scheme, but may be unaware of the origin of the money. Depending on the capabilities of the criminal actors, they may use a whole network of money mules, thus breaking the direct link between the victim and the final recipient.

- ▶ Some of the bank accounts used in the misleading invoice fraud have been detected in other types of frauds, such as 'shock calls'³⁰. In light of the hiring of money mules, criminal networks are specialised in offering bank transfer logistics that can be used for auxiliary criminal activities for redirection of funds obtained as a result of these activities.
- ▶ Fraudsters use the services of virtual banks that offer virtual IBANs. Virtual banks registered in the EU provide the possibility for all residents in the European Union to open a bank account.
- ▶ In recent years, the use of Egyptian and Kazakhstani IBANs has increased. In most of the cases, the origin of the bank account is a sign for the recipients of the misleading invoices to withhold from transferring requested fees. In other cases, the victims' banks need additional authorisation and automatically block the payments. Nevertheless, the fraudsters are aware that if the transfer is successful, a coordinated international investigation of the scam would be difficult and time consuming.
- ▶ The fraudsters use bank accounts as a first level in the chain for moving the funds. It is also assessed that subsequent transactions may occur involving crypto-currency exchanges.

³⁰ Fraudsters contact their victims over the phone introducing themselves as police officers and claim that a relative of the victim (in most cases a son or daughter) has been involved in an accident or is in custody and needs money to be released or to pay for the damage caused. Mainly elderly people are targets.

The way forward

Warning! From email spoofing to phishing attacks

Spoofing EUIPO's official email may be considered as the first stage of involving the Office in the area of cyber-enabled fraud. Email spoofing techniques are an inseparable part of the phishing attacks that aim at stealing data from the victims – personal data or, in most cases, data related to bank accounts. Additionally, phishing is most commonly executed through fake emails, websites and data collection portals. The scammers who commit the misleading payment request fraud have already developed a well-organised infrastructure with all the necessary elements that can be successfully implemented and exploited in phishing attacks – bank accounts, emails, websites, victims expecting to be contacted by an official authority.

Obtaining IPR applicants' and owners' email addresses from open internet sources and officially published information related to their IPR, may be misused by the fraudsters and support them in the development of this criminal scheme. Europol analysis shows that they are contacted before the IPR registration process is complete, when they are most vulnerable. The victims are expecting an answer from the competent IPO, so emails with attachments are not unexpected. What is more, they are eager to follow any instructions and comply with any requirements of interest in getting their IPR registered. The fraudsters may take advantage and use this scenario to manipulate the victims with the sole purpose of taking control over their bank accounts, thus causing even greater financial losses.

How should recipients of misleading payment requests act

In most cases, recipients of misleading payment requests who noticed the scam did not pay the requested fees. Following their intuition, they immediately got rid of the misleading invoice or deleted the fraudulent email without filing a complaint with the competent local LEA or notifying the respected national or international IPO.

In some cases, victims paid the requested fee, but discovered in time that they were being defrauded and withdrew the bank transfer – timing is essential to have a chance to retrieve the funds in these situations.

However, when a misleading payment request or any other related communication is received, there are several steps that must be followed before paying the requested fee:

- ▶ Double-check the legitimacy of the company. As mentioned, EUIPO's official webpage provides up-to-date information on the new companies suspected to be involved in misleading payment requests. A simple search of the company name on the internet may result in information regarding its legitimacy.
- ▶ Check the authenticity of the services offered – the whole text of the letter must be read and understood, as it provides information for the reason of the request: is it an offer, is it a proposal for signing a contract, is it an informative

message or an invoice?; are the services offered real and needed by the recipient?; do they overlap with the protection offered by EUIPO?

- ▶ Check the legal basis for the requested payment and who the beneficiary is: is the fee requested due in accordance with a national law or EU regulation? For what service and to whom will the fees be transferred?
- ▶ Check the origin and the authenticity of the bank account – the only two official EUIPO bank accounts are ES03 2100 2353 0107 0000 0888 and ES08 0049 6659 0121 1622 4792. A request for payment to the EUIPO that comes with bank account details different from these is a clear sign of a scam. Additionally, there are various websites that provide information on the authenticity of IBANs³¹.

Any actions taken to comply with requests in the correspondence without checking that the information is correct in advance entail a high risk of the recipient being defrauded.

IPR owners/applicants can protect themselves from becoming victims of misleading payment request frauds and phishing attacks in general by keeping in mind the following.

- ▶ Always check email headers (the header contains the email's metadata – sender, receiver, route of the email, timestamp).
- ▶ In most phishing attack cases, there is a difference between the sender's display name and the actual email from which it was sent, which is a clear sign of attempted fraud. Europol analysis shows that fraudsters carrying out in impersonation fraud register domain names that imitate the genuine domain name of the impersonated entity, but have slight misspellings or additional characters or words.
- ▶ Make an overall assessment of the email content: use of informal language; spelling mistakes or grammar errors; addressing the recipient inaccurately, impersonally or generically; requests for urgent payments with short deadlines that create a feeling of anxiety and worry.
- ▶ If the content of the email is suspicious, any attachments must not be downloaded, QR-codes must not be scanned or links clicked on.

Many recipients decide that deleting the email or discarding the letter and the envelope are enough to keep them safe from scamming attempts. On the contrary, all communication should be kept/downloaded and reported to the local competent police unit or prosecutor's office. The competent national or international IPO should also be notified. Reporting the scam enables the public authorities to get a clear idea of the dimensions of this international crime phenomenon.

³¹ https://www.ibancalculator.com/iban_validieren.html

Europol and the Anti-Scam Network

EUROPOL in close collaboration with EUIPO, the Anti-Scam Network members and European law enforcement authorities, has been monitoring and analysing the trends and the developments related to misleading payment request frauds since 2015.

On a regular basis, EUIPO sends datasets with information provided by IP system users. This information includes misleading invoices and payment requests received post or email, along with all available communication between the victims and the fraudsters. This data is analysed in detail, crosschecked against the Europol databases and OSINT research is then conducted in order to enrich and develop the available data. The results of the analysis and OSINT research are disseminated in the form of intelligence packages to the competent LEA in the MS and to Europol's operational partners. This is important, given the fact that countries in Asia, South America, North America and Australia have operational agreements on the exchange of operational data with Europol. The purpose of this step is to update partners on the crime situation related to this specific cross-border fraud scheme and raise awareness internationally. Furthermore, the operational information shared by Europol can be used as a basis for opening investigations in accordance with the recipient's national legislation.

Europol facilitates international cooperation between police forces by organising operational meetings and bringing together the leading investigators of ongoing investigations relating to misleading invoice and payment request frauds. Establishing direct contact between the investigators and providing the proper environment for exchanging of operational information and sharing experiences and best practice, increases the efficiency of the competent authorities' investigations.

In parallel with the operational perspective, Europol acts on a strategic level with the relevant stakeholders of the Anti-Scam Network – user associations, national and international intellectual property offices. These entities are the first point of contact with IPR applicants when it comes to the IP registration process. Exchanging experiences and information about weak spots and vulnerabilities in the process that can be exploited and misused by fraudsters allows them to improve their way of working.

International and inter institutional cooperation is key to successfully combatting this serious organised crime phenomenon.

Recommendations

- ▶ Awareness campaigns among all customers of competent international and national organisations responsible for IP registration and protection. Users be aware that once they file an application for an IPR registration, they become a potential target for scammers. It is recommended that these campaigns be held regularly, using appropriate channels to reach out to customers and provide clear information on risks that IP users may face and countermeasures that can be taken. In particular:
 - the authenticity of every communication must be double-checked, especially when it contains a payment request;
 - the IBAN is the only element of the fraud scheme that cannot be manipulated by fraudsters. Every intellectual property office should highlight and promote their official IBAN/s;

- if they receive a misleading invoice or payment request, recipients should report the fraud to the competent local police unit or prosecutor's office and then to the EUIPO Business Support Department.
- ▶ Improve cooperation between LEAs and regional internet registries and international organizations like RIPE NCC (Reseaux IP Européens Network Coordination Centre³²) and ICANN (Internet Corporation for Assigned Names and Numbers³³). These organisations could assist investigations with a cyber element, given that they own a huge database with intelligence related to IP addresses, domain name registrars and registrants.
- ▶ To efficiently counteract this organised cross-border criminal scheme, cooperation between the competent LEAs can be enhanced with the help and the support of Europol.
- ▶ Enhance the involvement of the national IPOs and provide a solution for the fast exchange of information about new trends, countermeasures taken to prevent scams, good practices and experiences.

³² Independent, not-for-profit membership organisation that supports the infrastructure of the internet through technical coordination in Europe. It helps to maintain a well-organised and efficient internet, and also to safeguard the numerous resources in use. Available (2024) at: [What We Do — RIPE Network Coordination Centre](#)

³³ Not-for-profit association which includes members from all over the world dedicated to keeping the internet secure, stable and interoperable. It promotes competition and develops policy on the internet's unique identifiers. Available (2024) at: [What Does ICANN Do? - ICANN](#)

List of abbreviations

AI	Artificial Intelligence
BOIP	Benelux Office for Intellectual Property
DPMA	Deutsche Patent- und Markenamt (German Patent and Trademark Office)
EIPS	European Intellectual Property Services
EUIPO	European Union Intellectual Property Office
EUTM	European Union Trade Marks
ICANN	Internet Corporation for Assigned Names and Numbers
IOCTA	Internet Organised Crime Threat Assessment
IP	Intellectual Property
IPO	Intellectual Property Office
IPR	Intellectual Property Rights
KYC	Know Your Client
LEA	Law Enforcement Authorities
MS	Member State
RIPE NCC	Reseaux IP Européens Network Coordination Centre
STR	Suspicious Transaction Report
TLD	Top-level Domain
UIBM	Unfficio Italiano Brevetti e Marchi (Italian Patents and Trademark Office)
VPN	Virtual Private Networks
WIPO	World Intellectual Property Organization
WPTR	World Patent and Trademark Register