EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

EMPACT

Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases

Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases

ISBN: 978-92-9156-356-2 Catalogue number: TB-09-24-179-EN-N: DOI: 10.2814/279888
© European Union Intellectual Property Office, 2024
Reuse is allowed provided the source is acknowledged and changes are mentioned (CC BY 4.0)

General disclaimer

This guide is not intended to give legal advice and does not supersede, nor is it meant to substitute the requirements of national law, international law, or any government regulations, policies, or priorities.

Acknowledgments

The EUIPO contracted with a research team of the United Nations Interregional Crime and Justice Research Institute (UNICRI) to develop this guide. The research team consisted of John Zacharia, Mariana Diaz Garcia, and Marco Musumeci. In addition, Erling Vestergaard from the EUIPO, greatly contributed to the drafting of the guide.

This report was made possible thanks to the invaluable insights and expertise of a number of experts, including:

Ankit Sahni, Ann Charlotte Söderlund, Antonio Bana, Barbara Suhr-Jessen, Bram Debusscher, Bruce Foucart, Carina Gommers, Constantin Rehaag, Cristopher Chillemi, Dani Bacsa, David Gilmore, David Wurgler, Dusko Martic, Elio de Tullio, Filip Kovc, Graeme Grant, Gytis Brazauskas, Iuliia Kozak, Jason Kosofsky, Johan Bravert, Juna Shehu, Laetitia Lagarde, Macarena Alvarez, Mar Peire Nadal, Marcin Fijałkowski, Maria Cecilia Romoleroux, Marie Amstrup Jensen, Marie-Ange Boyer, Melissa Morgia, Michael Lund, Mladen Vukmir, Nicola Novaro, Pascal Hetzscholdt, Reece Wickens, Riccardo Castiglioni, Sara Tarantini, Stefan Sergot, Steven Salway, Tom Peperstrate, Tuomas Kannas, Vladimir Marenovic, Wilfred Rogé, Zeegar Vink, Zoltan Kovesdi and Zoltan Varga.

Disclaimer: the views expressed in the report cannot be attributed directly to any interviewed or contributing expert.

Call for contributions

The EUIPO welcomes any suggestions or ideas that could add to or improve the fight against intellectual property crime. If you would like to comment or contribute, please send an email to:

observatory@euipo.europa.eu

Table of contents

Foreword

In 2012, the Observatory on Infringements of Intellectual Property Rights was entrusted to the EUIPO to provide facts and evidence to support effective intellectual property (IP) policies, create tools and resources to aid in the fight against IP infringements, and raise awareness of the importance of IP, a well-functioning IP protection and registration framework, and the negative effects of counterfeiting and piracy. A key focus of the Observatory during the past almost 12 years has been to build capacities and share good practices amongst law enforcement officials, prosecutors, IP owners and other stakeholders in the IP crime enforcement eco-system.

As the European Union Serious and Organised Crime Threat Assessment (EU SOCTA) policy cycle 2022-2025 comes to an end, a guide to criminal referrals in IP crime cases can be presented. The guide is one of the results of over 2 years of work carried out by the Observatory in support of the EMPACT priority.

The guide is built on interviews with practitioners from all over the world and extensive case reviews. It provides a much-needed collection of experiences, advice and good practices with the aim of improving the quality of criminal referrals in IP crime cases – particularly criminal trade mark counterfeiting, criminal copyright infringement, and trade secret theft cases. The EUIPO will also publish an in-depth analysis of IP crime legislation in the EU that will undoubtedly serve as a strong companion to this guide.

This guide serves as the public facing complement to the IP Crime Investigations Handbook that EUIPO first made available for law enforcement and judicial authorities in 2022. The guide helps IP owners who are victims of IP crime learn how to prepare and present criminal referrals to law enforcement. The guide further establishes a common framework for investigators and IP owners as to what information should be included in a criminal referral and, importantly, why this information is needed. In this way, it is hoped that the guide will become a resource for IP owners and investigators throughout the world.

João Negrão

Executive Director

EUIPO

Executive summary

Criminals recognise the value of intellectual property (IP), and they seek to exploit this value illegally through the trafficking of IP-infringing goods, the infringement of copyright-protected digital content, the theft of trade secrets, or other IP infringing activity. When IP owners are confronted with serious, mostly wilful, IP infringement, often on a commercial scale, they may choose to refer the case to a public investigating authority for criminal enforcement.

This *Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases* sets out a roadmap to assist IP owners who choose to refer cases involving the infringement of their respective IP to investigating authorities for criminal enforcement. The guide is built on extensive data collection, including, the expertise of the authors, case reviews, desk research, and more than 50 expert interviews. These experts included a broad range of IP owners, trade associations comprised of various IP owners, and public authorities who work with IP owners.

The guide is designed to be a practical, IP owner-focused tool to assist all IP owners in making a criminal referral of an infringement of their IP. The guide focuses on serious and often organised crimes involving trade marks, copyright and trade secrets, although most of the suggestions in the guide will also be relevant for infringements of other types of IP (e.g., registered or unregistered design rights). The special focus on trade marks, copyright and trade secrets reflects that these IPs are the most common in criminal proceedings.

A successful criminal investigation and subsequent prosecution of an IP crime depends, in a meaningful part, on substantial assistance from IP owners. Often, the IP owner is the first to notify investigating authorities of an IP crime – and that notification typically comes in the form of a criminal referral.

An important purpose of this guide is to make it easier for IP owners to provide important information to investigating authorities as part of their criminal referral. This guide will assist IP owners on how to conduct a preliminary investigation of an IP infringement in preparation for a criminal referral as well as how to prepare the criminal referral itself. In addition, the guide offers specific advice tailored to the three most common IP crimes: criminal trade mark counterfeiting, criminal copyright piracy, and trade secret theft.

The guide also provides sections intended to help IP owners understand their role after a public investigating authority has received a criminal referral and decided to open a criminal investigation. The IP owner can play a significant role during both a criminal investigation and public prosecution of an IP crime and during court proceedings. This role may vary depending on the type of IP crime involved. The guide endeavours to highlight and to explain the differences between the role of a trade mark, copyright, or trade secret owner during the different phases of a successful criminal investigation and public prosecution of an IP crime. The guide also offers factors for IP owners to consider at the end of a criminal IP case, such as preserving and storing evidence for a potential, parallel or subsequent civil IP case.

Moreover, the guide includes a helpful annex with checklists for IP owners to use when reporting a trade mark crime, criminal copyright infringement, and criminal trade secret theft. The checklists may be particularly helpful to small and medium-sized enterprises that may be making a criminal referral of an IP case for the first time. In the same vein, this guide also provides a brief description of the differences between different types of IP crime as well as a common international framework for when an IP infringement may constitute an IP crime.

Answers to 8 questions frequently raised concerning IP crime cases and the role of the IP owner are given below.

1. Is IP infringement always a criminal offence?

Whether a particular infringement of an IP constitutes a crime and satisfies the requirements for investigation and subsequent prosecution always depends on national legislation. In most countries, criminal penalties can be imposed on those who commit wilful trade mark counterfeiting and copyright piracy on a commercial scale, but many countries are also imposing criminal penalties on other types of IP infringement. For this reason, IP owners, private as well as public investigators, and prosecutors should be aware of national differences in the variety of IP crimes that may be investigated and prosecuted and how these differ depending on the country.

2. How does an IP owner determine whether a particular infringement of an IP warrants a criminal referral?

When deciding whether to make a criminal referral, IP owners may consider several factors – especially those that investigating authorities prioritise in deciding whether to accept a criminal referral for investigation. IP crimes with the highest impact on the IP owner and the public often warrant a criminal referral because they are most likely to be a high priority for investigating authorities. For example, IP crimes implicating public health and safety typically warrant a criminal referral. An organised crime group being responsible for the particular IP crime is another factor that weighs heavily in favour of making a criminal referral. Sometimes, the IP owner will also choose to make a criminal referral if the means necessary to investigate the IP crime is only available to a public investigating authority.

3. Where does an IP owner report a suspected IP crime?

In most cases, countries use their own national authorities to investigate and prosecute IP crimes, generally through the police and the public prosecution service. These national authorities usually have specific mechanisms in place for reporting and investigating IP crimes within their jurisdiction. Reporting IP crimes to the relevant national authorities is the main step in initiating the legal process and enforcement actions. Once a national authority accepts a criminal referral for investigation, the case will usually involve the public investigating authority choosing an investigation strategy, conducting a preliminary investigation, executing a search or multiple searches on an ‘action day’, finalising the investigation, followed by an indictment and the court proceeding itself.

4. *What information can an IP owner gather as part of its private preliminary investigation for possible inclusion in a criminal referral?*

Although a private preliminary investigation conducted by an IP owner is not a substitute for a formal criminal investigation, the IP owner can use a private preliminary investigation to gather important information. During this private preliminary investigation by the IP owner, several broad categories of information could be gathered, such as an analysis of the infringing item(s) obtained through a test purchase, financial information related to the purchase, and identifying information attributing the IP crime to a particular group or individual. Information can be gathered by IP owners through various methods and from various sources. This can be achieved through multiple strategies, such as observing or monitoring suspected illegal activity, and conducting a lawful online investigation into suspected IP criminals to obtain open-source intelligence (OSINT) and social media intelligence (SOCMINT). IP owners sometimes retain professional investigation services and specialised lawyers or firms to assist in gathering this information.

5. *What information can an IP owner include in a criminal referral?*

The initial referral package should contain sufficient detail to identify the IP owner and other victims of the crime, explain what crimes are involved, where and when the crimes occurred, who (if known) committed the crimes, why the IP owner chose to refer this particular case, and why investigating authorities should accept the referral for investigation. Although it is not usually necessary to include every conceivable detail, IP owners often offer to provide more complete details to investigating authorities at their request. In cases where the investigating authority is not familiar with IP crime, the criminal referral can contain an explanation of IP related issues, including an explanation of how the national IP laws may apply to the IP crime in the criminal referral.

6. *How does an IP owner's behaviour change after making a criminal referral?*

How an IP owner's behaviour may change after making a criminal referral may depend on the targets of the IP investigation. An IP owner may not wish to send a cease-and-desist letter or a takedown notice after deciding to make a criminal referral – although the IP owner might otherwise do so in the normal course of confronting infringers – because the IP owner may not want to 'tip-off' the targets that they are under investigation. Similarly, investigating authorities may advise IP owners that they are considering a criminal investigation and may ask the referring IP owner not to take any action that may alert the targets that they are under scrutiny. On the other hand, the targets of the IP investigation may very well be the subject of a criminal referral precisely because the targets have already received dozens of cease-and-desist letters or takedown notices and have chosen to ignore them. In this situation, an IP owner's behaviour may remain unchanged.

7. *What is the role of an IP owner during the criminal investigation and the court proceedings?*

Once the criminal investigation has begun, it is unlikely that the IP owner's role will end. When investigating authorities conduct searches to obtain evidence, they will often rely on IP owners to assist in evaluating this evidence. In some instances, IP owners will be given access to the seized evidence after the fact, and they can help investigating authorities correctly identify the

infringing items, distinguish between types of infringing items, and gain a better understanding of the evidence that they have seized. If the IP owner has conducted a test purchase, investigating authorities may ask IP owners to provide documentation establishing the chain of custody for the test purchase or download. IP owners can also continue to play a role in an IP crime case after the commencement of court proceedings. The role of the IP owner can become particularly important during evidentiary hearings, trials, and sentencing hearings when IP owners testify as witnesses. IP owner testimony can be broad in scope – touching on almost every element of the IP crime at issue.

8. Can an IP owner claim damages during a criminal proceeding?

In many cases, the IP owner can make a claim for civil damages (often called 'restitution') as part of the criminal proceeding – usually during or after the sentencing phase. Many jurisdictions even authorise IP owners to bring a civil proceeding for damages in parallel to the criminal proceeding. More often, jurisdictions authorise IP owners to bring a civil proceeding for damages against an IP criminal after the criminal prosecution has ended. In anticipation of this type of civil proceeding, it is important for an IP owner to ensure that any evidence used in the criminal proceedings that the owner may need for a subsequent civil claim for damages is preserved. Typically, either the public prosecutor or the IP owner will file a formal motion or request asking the judicial authority overseeing the criminal proceeding to preserve any evidence needed for a later civil proceeding for damages.

As reflected in the interviews with IP owners and their representatives, several good practices have been identified, including the advantage of establishing trustworthy brand protection procedures within the company, such as regular market monitoring to collect data, information intelligence, and evidence. Cooperation between IP owners through trade associations is often helpful in this regard.

In addition, IP owners and their representatives have also identified several obstacles to effective enforcement, including the low priority sometimes given to IP crime, a potentially insufficient legal framework, and jurisdictional challenges, especially in the online environment.

Definitions

Copyright and related rights: a legal concept that grants the creator of an original work exclusive rights to control the use and distribution of that work for a certain period. This means that others cannot reproduce, distribute, or perform the work without the creator's permission. Copyright protection covers a wide range of creative works, including literature, music, art, and software. Closely connected to copyright is the protection of performing artists during their performances, producers of phonograms in their recordings, broadcasters in their radio and TV programs, and other related rights.

Copyright piracy: commonly, copyright piracy refers to clear-cut unauthorised infringement of original creations, such as literary works, sound recordings, audio-visual works, computer software, and applied arts (e.g., original designs of customer goods and handicraft). Pirated copyright goods are copies made (a) without the consent of the IP owner(s); (b) directly or indirectly from an original article or work; and (c) where the making of that copy amounts to copyright infringement, or, in the case of imported goods, would have done so if performed within the jurisdiction.

Counterfeiting: although the term 'counterfeiting' is often used to refer to the unauthorised appropriation of various types of IP, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) uses it only to refer to trade mark infringements. A counterfeit mark is identical to or indistinguishable in its essential aspects from a protected trade mark. The elements in question depend on the terms of national law, but the requirements for criminal prosecution discussed in this handbook are these: the trade mark must be registered within the local jurisdiction; the defendant must use a counterfeit mark; the counterfeiting must be on a commercial scale; and the counterfeiting must have been committed wilfully.

Counterfeit trade-marked goods: Footnote 14 to Article 51 of the TRIPS Agreement states that 'counterfeit trade-marked goods' means any goods, including packaging, bearing, without authorisation, a mark that is identical to a trade mark validly registered for those goods, or that cannot be distinguished in its essential aspects from such a trade mark, and that thereby infringes the rights of the owner of the trade mark in question under the law of the country of importation.

Cyberattack: an action that includes unauthorised access to an information system, interference with an information system or unauthorised data interception and misuse of certain devices. The most important international legal instrument concerning cyberattacks is the Cybercrime Convention.

Cyberfraud: a type of criminal act committed online using electronic communications networks and information systems to commit online fraud or forgery. Large-scale fraud can be committed online using techniques such as cybersquatting, typosquatting, identity theft, phishing, spam, and malicious code. The most important international legal instrument concerning cyberfraud and cyberforgery is the Cybercrime Convention.

Cybersquatting: a term usually used to describe the unauthorised registration and use of a domain name that is identical to another's trade mark.

Infringement of intellectual property (IP): a term that covers directly IP-infringing acts as well as (for the purposes of this guide) contributory and preparatory acts in furtherance of conspiracies and attempts to commit IP infringement and other closely related illegal acts or criminal offences (e.g., cybercrime offences and money laundering).

Intellectual property (IP): creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce to identify the origin of goods and services, plant varieties, geographical indications, and commercial secrets. IP is protected in various international legal instruments and national laws. For criminal proceedings, the most important IPs are copyright and related rights, trade marks, and trade secrets.

Intellectual property (IP) crime: IP crime depends on national legislation. The only international (or EU standards) concerning IP crime are the provisions in Article 61 of the TRIPS Agreement concerning wilful trade mark counterfeiting or copyright piracy on a commercial scale, and Article 10 of the Cybercrime Convention concerning crimes related to infringements of copyright and related rights.

Organised crime group (OCG): a group of three or more persons existing over a given period and acting in concert with the aim of committing crimes for financial or material benefit, according to the definition adopted in the United Nations Convention against Transnational Organized Crime (2000). This definition does not preclude investigations of two or more persons for conspiracy to commit an IP crime. This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 in the fight against organised crime.

Pirated copyrighted works: Footnote 14 to Article 51 of TRIPS states; 'pirated copyright goods shall mean any goods which are copies made without the consent of the IP owner or person duly authorised by the IP owner in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation'. Although the definition in TRIPS refers to 'goods', it applies equally to the piracy of online copyrighted works.

Trade mark: a sign, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, or a combination of these elements, provided that that such signs are capable of distinguishing the goods and services of one undertaking from those of other undertakings (see a link to EU trade mark legislation to the right). A trade mark can serve to identify and distinguish the goods or services of a particular company or individual from those of others in the marketplace. Trade marks help customers easily recognise products or services with a particular brand or source. In addition, trade marks can be registered with the state to provide legal protection against unauthorised use by others, and are important for businesses because they help build brand recognition and reputation.

Trade secrets: According to European Union Directive 2016/943, a trade secret is information that meets all of the following requirements:

- it is secret, in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret;
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Typosquatting: a term usually used to describe the unauthorised registration and use of a domain name that is similar to another's trade mark.

I Introduction

I.A Context

Intellectual property (IP) plays an ever increasing and significant role in the global economy, protecting some of the most valuable intangible property in the world. IP owners include pharmaceutical companies developing vaccines under trade mark protected brand names to protect global health, universities and other entities developing scientific breakthroughs protected as trade secrets, content industries creating copyright protected music, movies, and video games, and so much more.

Information on the contribution of IP intensive industries in the European Union can be accessed by clicking on or scanning this QR code.

Criminals operating throughout the world also recognise the value of IP and seek to exploit this value illegally through the trafficking of IP-infringing goods, the infringement of copyrighted works, and the theft of trade secrets. Criminals also may commit related crimes such as cybersquatting or typosquatting fraud, money laundering, computer hacking, and other cybercrimes in the course of committing an IP crime. When IP owners are confronted with the counterfeiting, infringement, or theft of their IP and wish to enforce their IPs, some will file a civil case or initiate a private criminal prosecution. Others will refer the case to a public investigating authority for criminal enforcement. It is the latter choice – referral for public criminal enforcement – that provides the context for this guide.

I.B Background and purpose of the guide

In 2021, the European Union's Council of Ministers included IP crime among the top priorities in the fight against organised crime for 2022-2025. These will be addressed through the European Multi-disciplinary Platform against Criminal Threats (EMPACT), a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime.

Information on the EMPACT decision can be accessed by clicking on or scanning this QR code.

The ten priorities that have been identified for 2022-2025 are the following:

1. high-risk criminal networks;
2. cyberattacks;
3. trafficking in human beings;
4. child sexual exploitation;
5. migrant smuggling;
6. drug trafficking;
7. fraud, economic and financial crimes;

8. organised property crime;
9. environmental crime;
10. firearms trafficking.

EMPACT Priority 7 targets fraud, economic and financial crimes. In its Aim 4, which is specifically related to IP crime and counterfeiting of goods and currencies, it proposes, inter alia, 'to combat and disrupt criminal networks and criminal individual entrepreneurs involved in IP crime and in the production, sale or distribution (physical and online) of counterfeit goods or currencies, with a specific focus on goods harmful to customers' health and safety, to the environment and to the EU economy'.

Through EMPACT, the EU has adopted an integrated approach to its internal security, involving measures that range from external border controls, police, customs and judicial cooperation to information management, innovation, training, prevention, and the external dimension of internal security. It is an intelligence-led and EU Member State-driven cooperation instrument that allows Member States, agencies, and other actors to work closely together to address key criminal threats, using tools such as law enforcement training and joint operations to dismantle criminal networks and their structures and business models.

EMPACT works with the General Multi-Annual Strategic Plans (MASPs) across Common Horizontal Strategic Goals for all the Operational Action Plans (OAPs) that will be implemented. This approach aims to strengthen consistency and coherence among OAPs as well as the multi-disciplinary and multi-agency approach.

The driver of OAP 7.4 was Bulgaria, with Italy, Spain, and Portugal as co-drivers. The operational action leader of the guide was the EUIPO, with EUROPOL as co-leader.

Fourteen EU Member States participated in the guide operational action in 2023: Belgium, Bulgaria, Cyprus, Denmark, Germany, Greece, Hungary, Ireland, Malta, Netherlands, Portugal, Romania, Spain, and Sweden. Several third countries also participated in 2023: Albania, Moldova, North Macedonia, Serbia, Switzerland, and the UK.

In this context, the EUIPO actively supports the implementation of this priority within the EMPACT framework. As part of that implementation and in its role as the operational action leader, the EUIPO contracted with a research team of the United Nations Interregional Crime and Justice Research Institute (UNICRI) to develop this guide.

The purpose of this guide is to assist the owners of trade marks, copyrights, and trade secrets who choose to refer cases involving the infringement of their respective IPs to investigating authorities and public prosecutors for criminal enforcement. IP crimes cannot be effectively investigated and prosecuted without substantial assistance from IP owners. Investigating authorities often cannot investigate an IP crime unless the IP owner notifies investigative authorities of such crimes through a criminal referral. As a result, another purpose of this guide is to make it easier for IP owners to provide important information to investigating authorities.

This guide focusses on five topics:

- conducting a preliminary investigation of an IP infringement;
- preparing a criminal referral;

- role of the IP owner during the criminal investigation;
- role of the IP owner during court proceedings;
- factors to consider after court decisions.

The guide also includes an annex with checklists for reporting a trade mark counterfeiting crime, criminal copyright infringement, and criminal trade secret theft.

I.C Methodology

Although many of the largest IP owners are not new to the criminal referral process, many new IP owners, and small and medium sized enterprises (SMEs) have never referred an infringement of their IP for criminal enforcement. The guide is designed to be a practical, IP owner-focused tool to assist all IP owners in making a criminal referral of an infringement of their IP.

To that end, the guide relies principally on the expertise of the authors and on the interviews of more than 50 experts. These experts included a broad range of IP owners, trade associations comprised of various IP owners, and public authorities who work with IP owners.

The guide is designed to be a practical, IP owner-focused tool to assist all IP owners in making a criminal referral of an infringement of their IP. The guide focuses on serious and often organised crimes involving trade marks, copyright and trade secrets, although most of the suggestions in the guide will also be relevant for infringements of other types of IP, e.g., registered or unregistered design rights (see a link to EU design legislation to the left). The special focus on trade marks, copyright and trade secrets reflects that these IPs are the most common in criminal proceedings.

Copyrights and related rights

A legal concept that grants the creator of an original work exclusive rights to control its use and distribution for a certain period.

Trade marks

A sign, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, provided that that such signs are capable of distinguishing the goods and services of one undertaking from those of other undertakings.

Trade secrets

Information that (a) is secret in the sense that it is not generally known; (b) is commercially valuable because it is not publicly known; (c) has been subjected to reasonable steps to keep it secret.

I.D What are copyrights and related rights?

Copyrights refers to a legal concept that grants the creator of an original work exclusive rights to control the use and distribution of that work for a certain period. This means that others cannot reproduce, distribute, or perform the work without the creator's permission. Copyright protection covers a wide range of creative works, including literature, music, art, and software.

Not only whole works, but also their parts can be protected by copyright, as long as they are original. By analogy, unfinished or incomplete works may also be protected by copyright if they fulfil the originality requirement. The primary international copyright agreement is the Berne Convention for the Protection of Literary and Artistic Works which introduced the concept that protection exists the moment a work is 'fixed'. In other words, it exists the moment the work is written or recorded in some tangible medium. At that time, the author of the work is automatically entitled to copyright protection of the work and to any derivative works, unless and until the author explicitly licences or transfers them or until the copyright expires. Copyright is automatic and does not require formal registration, unlike other IP such as trade marks. The general rule is that copyright protection must be granted until the expiration of the 70th year after the author's death.

Closely connected to copyright is the protection of related rights, which cover the rights of performing artists in their performances, producers of phonograms in their recordings, broadcasters in their radio and TV programs and other related rights.

I.E What are trade marks?

A trade mark is a sign, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, or a combination of these elements, provided that that such signs are capable of distinguishing the goods and services of one undertaking from those of other undertakings (see a link to EU trade mark legislation to the left). A trade mark can serve to identify and distinguish the goods or services of a particular company or individual from those of others in the marketplace.

Trade marks help customers easily recognise and associate products or services with a particular brand or source. In addition, trade marks can be registered with national or regional authorities to provide legal protection against unauthorised use by others. The trade mark can also be registered in a special format, which could include stylised wording, special fonts, additional graphic elements or even distinctively shaped packaging. Finally, the trade mark is related to specific goods or services sold to the customers.

Trade marks are important for businesses because they help build brand recognition and reputation. In the same vein, trade mark counterfeiting causes the most harm to brand owners

and thus reflects the most serious forms of trade mark infringement and can be subject to criminal prosecution.

Well-known trade marks

Article 6bis of the 1967 **Paris Convention for the Protection of Industrial Property** requires member countries, to afford certain protections to well-known marks, regardless of whether they are registered. Article 16.2 of the **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement** extended Article 6bis of the Paris Convention to include services. It also provided that members shall take into account that a mark is well-known to a relevant sector. Article 16.3 extended the protections to well-known marks when used on unrelated goods or services in cases where the well-known mark is registered, if such use indicates a connection to the owner and the owner of the well-known mark would likely be damaged.

I.F What are trade secrets?

A trade secret is information that (a) is secret in the sense that it is not generally known among or readily accessible to persons who normally deal with that kind of information; (b) is commercially valuable because it is not publicly known; (c) has been subjected to reasonable steps to keep it secret. The efforts taken to maintain the information's secrecy are not definitively outlined in any legislation; whether the steps taken are reasonable is a matter for case-by-case consideration. Trade secrets do not require registration or examination and can last for an indefinite period of time (as long as the information is kept confidential and continues to have independent economic value). Hence, the unauthorised misappropriation of a trade secret constitutes a trade secret violation. Article 39 of TRIPS requires member countries to protect "undisclosed information" (*i.e.*, trade secrets) in the course of ensuring effective protection against unfair competition consistent with Article 10*bis* of the 1967 Paris Convention.

I.G When does an IP infringement constitute a crime?

I.G.1 International standards

The criteria for an IP infringement to constitute a crime and the specific international standards applicable to such an infringement are generally established through international agreements and treaties such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). TRIPS is an agreement administered by the World Trade Organization (WTO), which sets out minimum standards for IP protection and enforcement. It covers a wide range of IP,

including patents, copyrights, trade marks, geographical indications, industrial designs, and trade secrets. One hundred sixty-four countries are parties to TRIPS (all WTO members). TRIPS is the first and most comprehensive multilateral agreement on IP.

By ensuring that Member States offer efficient legal remedies and enforcement procedures against IP infringements, these guidelines seek to unify IP laws among various nations. However, specific aspects of implementation and enforcement usually vary among countries.

According to Article 61 of TRIPS, copyright piracy and trade mark counterfeiting that constitute a civil infringement may also constitute a criminal offence where the infringement is both wilful and carried out on a commercial scale.

Although TRIPS requires parties to the agreement to impose criminal penalties at least on those who commit wilful trade mark counterfeiting and copyright piracy on a commercial scale, countries are free to impose criminal penalties on wilful or knowing infringements of other types of IP. For example, many countries have chosen to impose criminal penalties on those who knowingly steal trade secrets. For this reason, investigators and prosecutors should be aware of national differences in the variety of IP crimes that may be imposed from country-to-country.

Article 61 of TRIPS states the following in relation to criminal procedures: *Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trade mark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.*

Copyright and related crimes perpetrated online can also fall under the larger scope of cybercrime as defined in the Budapest Convention on Cybercrime.

Article 10 of the Convention on Cybercrime states the following in relation to offences related to infringement of copyright and related rights: *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.*

I.G.2 National standards

Every country will have its own national standards implementing the TRIPS obligations and otherwise imposing criminal sanctions for criminal trade mark counterfeiting, criminal copyright infringement, trade secret theft, and other IP-related crimes. IP owners can reference the upcoming EUIPO study entitled 'Legislative Measures Related to Intellectual Property infringements - Phase 3: Criminal Measures in Serious and Organised Intellectual Property Crime Cases' planned for publication in mid-2024. This study aims to provide a comprehensive overview of the scope and substance of criminal measures related to IP-related crime in general. The study in particular focuses on significant legislative differences between jurisdictions and provides information on existing legislative limitations in the form of, for example, low to maximum sentencing options, limited availability of special investigation measures, high thresholds for investigations and prosecutions and occasional requirements for intent to deceive in counterfeiting cases.

I.H Where does an IP owner report an IP crime?

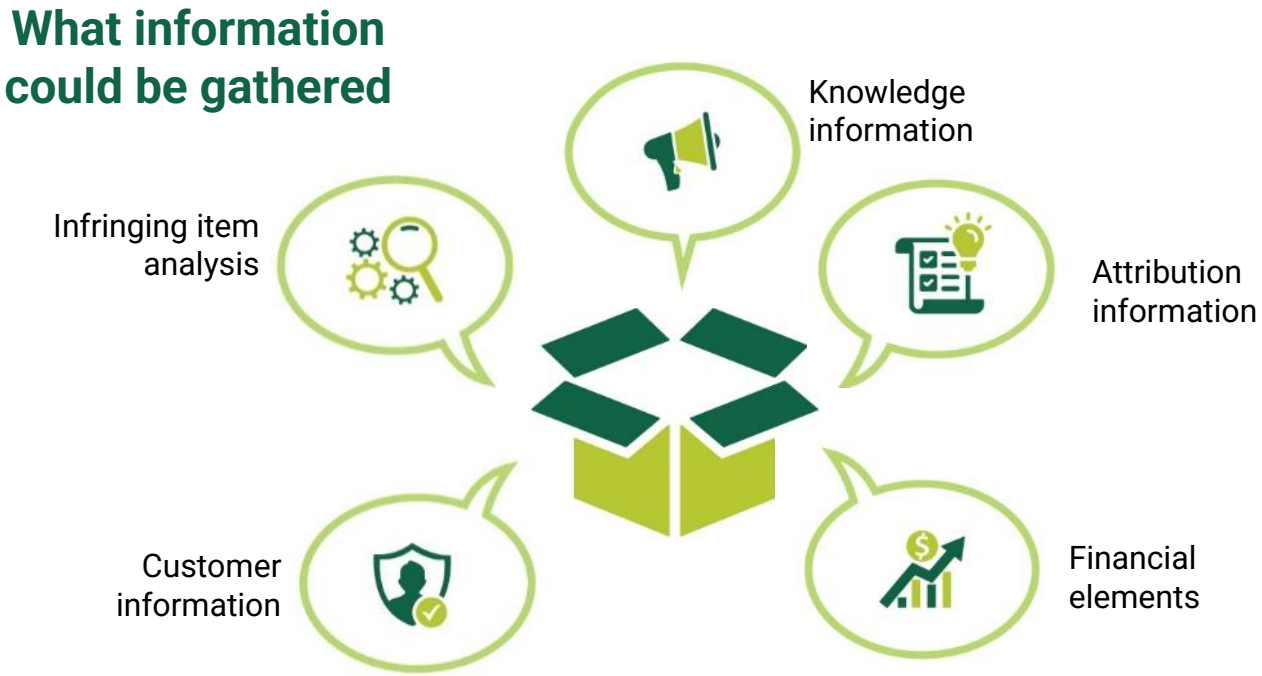
In most cases, countries use their own national authorities to investigate and prosecute IP crimes. These national authorities usually have specific mechanisms in place to report and investigate IP crimes within their own jurisdiction. Reporting IP crimes to the relevant national authorities is the main step in initiating the legal process and enforcement actions.

An overview of national institutions responsible for the investigation and prosecution of IP crimes by Eurojust can be accessed by clicking or scanning this QR code.

II Preliminary IP owner investigation

In the context of IP, an IP owner's preliminary investigation refers to the first actions taken to acquire data, information and evidence related to the discovery of a suspected infringement of its IPs. This investigation is usually conducted by the IP owner or their legal representatives and aims to determine the scope and nature of the potential infringement. There are some general components and guidelines that are normally found in a preliminary IP owner investigation, but these may differ based on the circumstances and the type of IP involved.

II.A Generally applicable guidelines



II.A.1 What information could be gathered

Sometimes an IP owner will carry out a preliminary investigation to support the criminal referral. It should be noted however that not all IP owners may have the capacity and expertise to conduct comprehensive investigations. In which case, it is sufficient to merely provide the information at hand in the criminal referral.

Although a preliminary investigation conducted by an IP owner is not a substitute for a formal criminal investigation, the IP owner can use a preliminary investigation to gather information and evaluate the strength of its case. This in turn can guide an IP owner's decision about any additional legal action, such as submitting a formal criminal referral, sending a cease-and-desist letter, or pursuing private litigation. During this preliminary IP owner investigation, several broad categories of information could be gathered, which can include a variety of elements helpful to establishing an IP crime, such as the following:

Infringing item analysis: Examining the allegedly infringing items (whether suspected copyright infringing items downloaded from the Internet or counterfeit goods purchased in a shop, market or online) being offered for distribution is helpful in establishing any IP infringement, including an IP crime. Analysing elements of the infringing item that might be covered by IP is also important. For example, analysing the packaging, labels, logos, design components, or other aspects of a counterfeit good obtained through a test purchase may be part of this process. IP owners are uniquely situated to identify those aspects of a test purchase that infringe their IP. By additionally analysing the content of a suspected copyright infringing item distributed online to confirm that it is indeed infringing, the IP owner can gather even more information. Again, IP owners are in the best position to confirm this type of information and if their IP have been infringed.

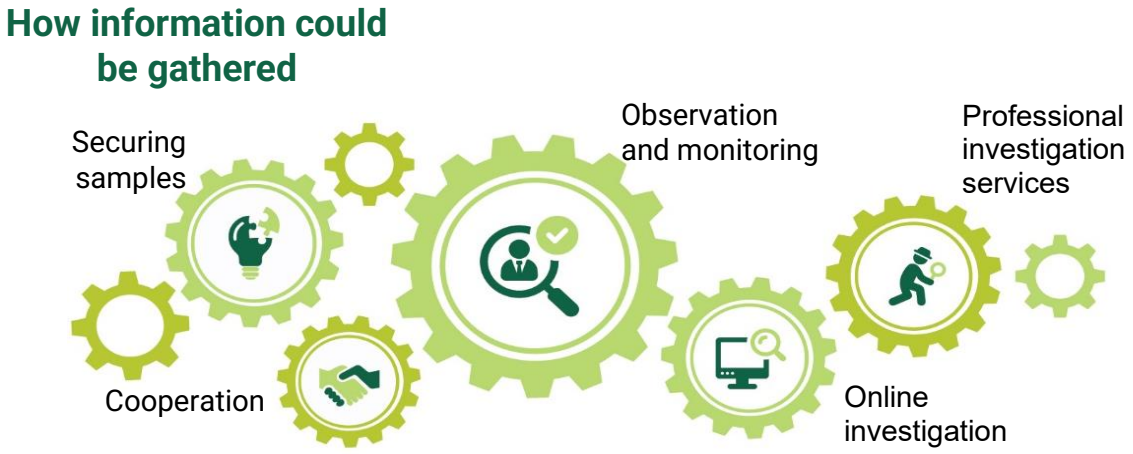
Customer information: Customer complaints can expose a seller who is distributing copyright infringing items or goods bearing counterfeit marks. More importantly, customer complaints can demonstrate the requisite wilfulness or knowledge of the IP criminal who chooses to continue distributing an infringing item after receiving a complaint. Sometimes customer complaints are made directly with the copyright or trade mark owner. At other times these complaints may be made by customers on an IP criminal's website or with online third-party marketplaces.

Financial elements: Analysing financial records and transactions stemming from a test purchase or download can provide evidence of illegal activities related to IP infringement as well as other crimes. This type of analysis may include tracking payments, invoices, bank statements, as well as identifying payment processors, brokers, host providers, and other financial documents to uncover the flow of funds associated with the infringing activities. This evidence can also be helpful in eventually establishing commercial scale and commercial purpose.

Attribution information: When conducting a test purchase, an IP owner may also gather information identifying the suspected IP criminal. For example, an online download of a copyright-infringing item may include metadata identifying the suspected IP criminal or organised crime group in which the criminal works. The suspected IP criminal may even

expose their IP address during an online transaction of an infringing item. In addition, the financial information provided by the seller of the infringing item may include financial elements that would expose the seller's true identity. In the context of the sale of counterfeit goods, sellers may even provide business cards, receipts, or other information that would facilitate identifying the seller.

Knowledge information. As noted above, Article 61 of TRIPS imposes criminal penalties for copyright piracy and trade mark counterfeiting that involves, *inter alia*, wilful conduct. Thus, during a preliminary investigation, IP owners can gather evidence establishing that a suspected IP criminal has wilfully engaged in an IP crime. For example, IP owners can gather copies of notice-and-takedown emails or cease-and-desist letters that the IP owner has sent to suspected IP criminals. IP owners can also gather evidence establishing receipt of such notices of conduct in violation of IP law. When customs authorities seize imports suspected of including goods violating IP law, they often provide simultaneous notice to both the importer and to the IP owner whose IPs, customs suspects, were infringed. IP owners can also gather these customs notices as part of their preliminary investigation. When an IP owner sees that a suspected IP criminal is offering an infringing item at an unusually low price, this too can suggest wilful conduct and can be evidence that the IP owner documents and gathers. Finally, IP owners can gather evidence of formal administrative or civil complaints filed by the relevant authorities or the IP owners themselves against suspected IP criminals notifying them that their conduct violated IP law.



II.A.2 How information could be gathered

Information can be gathered by IP owners through various methods and from various sources. The methods used to gather information will depend on the elements the IP owners need to prove and have the capacity to identify. This can be achieved through multiple strategies, such as the following:

- **Observation and monitoring:** Evidence of illegal activity can be obtained through observation and monitoring techniques. This could entail keeping an eye on suspicious activity in both physical and online spaces and documenting the results. Product analysis

and the identification of financial elements can be done through monitoring and conducting investigations. Monitoring can also be used alongside other analyses to understand the infringing business model and to identify other relevant elements that can help when preparing a criminal referral, such as the existence of clusters of IP owners affected by the infringement.

- **Online investigation:** Conducting online investigations can help to identify online platforms, websites, or social media accounts involved in the use or sale of infringing items. These investigations might involve different strategies such as monitoring online marketplaces, social media platforms, websites, and forums where infringing activities are suspected of taking place. This might include information about the accounts, IP addresses, or the content shared.
- **Professional investigation services**: Requesting the services of specialised investigators (usually, for an undercover investigation), specialised lawyers or firms experienced in conducting preliminary investigations. These professionals can assist in conducting due diligence and gathering relevant information. Such services can be procured to supplement investigations being conducted by an IP owner's in-house investigators, or these services can be used to conduct the entire investigation for an IP owner.
- **Securing samples:** Test purchases could be used to assess damages and to understand the nature of the infringement. This can be done directly by the IP owner or by professional investigation services. Importantly, samples or test purchases should be secured in a way that presumes that the sample or test purchase would someday be evidence in a criminal case. In other words, IP owners should carefully document the chain of custody for physical items and take screen shots and even online videos for online test purchases.

- **Cooperation:** Membership in trade associations can be helpful, as some associations gather information about suspected IP criminals on behalf of their members, especially when multiple members are victims of the same IP criminal. Establishing a good relationship with intermediaries such as online service providers or third-party online marketplaces can help IP owners gather information from these intermediaries. Trade associations also establish or facilitate cooperative relationships with intermediaries on behalf of the associations' members.

II.A.3 What types of intelligence and evidence could be secured

II.A.3.a Test purchases or downloads

Test purchases are utilised across various industries, but in the context of IP protection, they refer to the act of acquiring an item from a seller suspected of distributing copyright-infringing items or counterfeit goods. Customs interceptions, when coordinated with the IP owner, can be analogous to a test purchase. As already noted, test purchases can be used to either validate the

IP owner's suspicions or discover that the seller is indeed offering authentic products. For physical products, test purchase may uncover additional details such as financial information, shipping addresses and business names, that might not be easily accessible from a regular listing. This valuable information can aid in gathering intelligence about the individuals or entities involved in a counterfeit operation. For infringing items in digital form, test purchases, downloads, and streams can be used to confirm that a suspected infringing item is pirated, obtain the IP addresses of the websites used by the copyright criminal, and even obtain the criminal's own IP address.

IP Crime Case Example
To conduct its own investigation in a country, an IP owner contacted a partner software company in that sold the IP owner's software, asking them to conduct a test purchase from the defendants' online store. The partner company agreed and bought 30 units of the IP owner's software from the defendants' online store, then passed on the test purchases to the IP owner for testing. The partner also provided the IP owner with email correspondence with the defendants and the proof of payment related to the test purchases.

When conducting test purchases various aspects can be considered:

- When carrying out a test purchase, it is important to follow specific steps that will enable the correct documentation of the evidence that is being collected: for example, the information related to the infringing item such as the price appearance, payment methods, links to a jurisdiction, website language, currency, delivery options, who is purchasing, and the number of receipts, among other elements. There are differences between jurisdictions concerning test purchases and chain of custody. In some cases, purchases need to be done through an authorised person, whereas in others IP owners can do their own chain of custody process.

IP owners should monitor and document their actions – dates, what, where, when, screenshot, videography, so you have a visual representation. Investigation authorities find such content very convincing. Use locked files, emails, skype id, signal id, email, login etc. Don't stop with referral to the police, unless we are sure that police will take over the monitoring part, because if it takes a year, or more, hosting may change etc., a lot of evidence can be different.
– Private investigator of IP crime

- Preparing a comprehensive authentication report after the test purchase or several reports is one of the most relevant steps in a criminal referral. The IP owner can prepare a detailed report for internal purposes, a high-level document listing the characteristics that determine that the good is an IP-infringing good, and a more detailed report that has been reviewed internally, after the prosecutor requests more information. Notably, there are instances when the IP owner may not want to share all of its proprietary security features or forensic techniques with investigating authorities to prevent such information from entering the public domain. Nonetheless, IP owners should be prepared to provide an

expert or fact witness who can explain why an alleged infringing item is not an authentic copyrighted work or trade marked good. If it is impossible to establish that an item is infringing IP without revealing the IP owner's proprietary information, the IP owner can seek a protective order or other protective measures before disclosing the information.

One big part of the referral is the authentication report after the test purchase. Be careful to not disclose all your forensics, because it's going to be public.
– IP owner

IP Crime Case Example
Before filing the criminal referral, an IP owner conducted a series of analyses on the suspect cookie packages and their contents, identifying differences between the counterfeit products and the originals. To determine the product's composition, the IP owner sent the received samples to an accredited external laboratory for analysis. The results highlighted clear differences in the product's structure and composition. In particular, a difference in granulation and smell was noticeable at first glance. The analysis revealed significant differences in the formula, and specifically in the concentration of vitamins and nutrients. The external lab report stated that significant discrepancies were detected showing clear differences in the recipes used to produce the counterfeit samples. In particular, the nutritional values of the counterfeit samples were typical of any ground cookie that could be found on the market. The concentration of the vitamins varied, but it was significantly lower than the quantities contained in the original ground cookie.

- Gathering information about the financial details related to the test purchase to later include them in a referral.

Look at the payment processors, ad brokers, host providers, and then you can go to investigating authorities and say look, this is the money involved, number of people. Investigating authorities like big numbers.
– IP owner

- In more complex cases, where cross-border operations need to be performed or where a target is a high-profile infringer, it might be necessary to engage international investigators.

II.A.3.b Communication/information from customers

As mentioned above, customers can be a source of relevant information about a possible infringement. IP owners may receive complaints from customers who were scammed or deceived or are upset about the quality of the goods – thereby already providing initial pieces of evidence. In addition, customers can provide important elements for the investigation and criminal referral, such as the name and location of the unauthorised source and the process to acquire the goods or content.

IP Crime Case Example
A series of complaints from some of a beer company's customers about the quality of beer were received from café owners. These complaints provoked the beer company to analyse the external appearance of the kegs and their contents, whereupon the company discovered that the kegs did not contain the genuine beer. Best before stickers containing the number combination, indicating the place of origin of the kegs were also faked and had meaningless combinations.

IP Crime Case Example
An investigation started after an IP owner filed a criminal referral to the police about a branded food product, following a series of complaints from sellers who had recorded customers' dissatisfaction with the product. Customers living in the affected cities and areas had complained to shop owners and sellers operating in these locations following their purchases of the branded food product. Customers complained exclusively about the product's taste, as they had not noticed any difference in the packaging. The shop owners and sellers, in turn, complained to the IP owner about the same products and sent samples to the company. The IP owner had previously received complaints twice, and on both occasions, both the packaging and contents of the samples were analysed.

In some cases, IP owners have software or similar tools available to enable the customers to generate a direct report to the IP owner, or to analyse the product themselves before contacting them.

IP Crime Case Example
After experiencing some installation problems, a number of software purchasers, who had bought the products from the defendants in good faith, submitted them to the software owner to be checked. They also sent their invoices for buying these products, which demonstrated that they were purchased from the defendants.

Customers may also have emails or transcripts of online chats with suspected IP criminals that can help to establish the criminals' wilfulness or knowledge of the IP crime that they are committing. This can occur, for example, in response to a complaint about the quality of a counterfeit good or a customer query about why the prices of copyright infringing downloads or streams are so low.

II.A.3.c Observation

Monitoring the market can provide information about suspicious actor or activities. Some key pieces of information that an IP owner can gather during the monitoring stage include the following:

- Appearance, packaging, branding, and labelling of the infringing products. Often IP-infringing goods contain spelling mistakes on their packaging. IP criminals will sometimes use 'double packaging' whereby a good with packaging bearing counterfeit marks is packed inside another package that is generic and with no name, in order to avoid detection. Sometimes an IP owner can observe and identify inconsistencies between the packaging on the outside (*e.g.*, the box containing medicine) and the packaging on the inside containing the product itself (*e.g.*, child-resistant blister packs containing pills).

- Distribution channels through which infringing products are marketed and sold (retailers, distributors, wholesalers, online platforms, or any other channels involved in the distribution chain). This could provide information about other elements in the supply chain.

- Sales volume, pricing strategies, and discounts offered by infringers. This information could later be used by the IP owner to assess the commercial impact of the infringement and gather evidence for potential damages calculations.

- Information related to the alleged infringer, including accounts, personal information shared, or any indicator that could help identify the infringer.

- Geographical reach of the infringing activities. This information could be valuable when determining the extent of the problem and planning the steps ahead.

- Identification of advertisements, promotions, or marketing campaigns related to infringing products, including the information about the channels used.

- Parties involved in the infringing activities, such as manufacturers, importers, distributors, or sellers. This information could be valuable when initiating legal actions or sending cease and desist letters.

- Information that could allow the IP owner to identify when the suspicious activity related to the infringement started.

In some cases, IP owners can carry out the monitoring through private investigators or technology tools, including track and trace systems that can automate part of the process. Regardless of which techniques IP owners use for observation, it is helpful to document the actions taken and save the evidence found through the process, even after the referral is made.

IP Crime Case Example
An IP owners' private sector investigation organisation specialising in copyright investigations constantly monitors the commercial market of pubs and clubs airing sports events to ensure the use of approved and compliant technology from authorised providers and to make sure services are offered after having purchased an appropriate subscription. If they find evidence of illegal behaviour, they conduct their own investigation to collect evidence and to try and reconstruct the illegal supply chain of the fraudulent broadcast and of the fraudulent technology used to access it. The illicit streaming of TV programmes emerged during the preliminary phases of the case, and it became apparent through reports to and observations by industry, along with changes in subscription uptake, that behaviour in commercial premises such as pubs and clubs had changed and a detailed series of observations to investigate was undertaken.

IP Crime Case Example
A beer company, noticing decreasing numbers of orders from several cafés, asked café owners to examine several kegs. The beer company could see that best before stickers were fake, and that beer and keg caps were not original. The beer company demanded information from the caps manufacturer about who had ordered the fake caps. This led the beer company to the defendants. After which, an investigation agency was hired to observe the defendants. These observations revealed that the defendants, an active event organiser/caterer of the beer company, had initially ordered original beer kegs. However, once they were emptied, the kegs were not returned to the beer company, in direct violation of the General Terms and Conditions. Instead, the defendants cleaned the kegs on the outside, removed the original best before stickers and refilled the kegs with homemade beer that was not the beer company's beer. The defendants then sealed the kegs with caps that looked like the beer company's caps and resold the kegs as if they contained the beer company's original beer.

II.A.3.d Open-source intelligence (OSINT) and social media intelligence (SOCMINT) investigation

Open-source intelligence (OSINT) and social media intelligence (SOCMINT) is the practice of collecting and analysing information gathered from open sources and social media to produce actionable intelligence. This intelligence can support criminal investigation of IP crimes. OSINT/SOCMINT investigates open-source data collected for one purpose and then repurposes this data to identify patterns in behaviour, actors, or other elements. IP-infringing goods are often marketed or distributed in social media and online marketplace platforms, which provides an opportunity to apply OSINT/SOCMINT techniques to obtain relevant information.

Look at the social media accounts. From their own advertisements, you can get a sense of how long the infringer has been in business. It's a good indicator for a timeline.
– IP owner

Some techniques that can be used include the following:

- Using search engines to conduct online searches of social media platforms and online marketplaces to identify potential instances of infringement.

- Monitoring certain social media platforms to identify posts, profiles, comments, chats, or advertisements related to potential infringements. This can include following relevant hashtags and conversations, infiltrating private or closed groups in social media, and

examining interactions between users. The analysis can provide multiple indicators to identify the infringer and the modus operandi. In addition, creating undercover or false accounts (sometimes called 'sock puppets') can help in engaging with the infringer through the chat, messaging app, or other communication channels by pretending to be a potential customer. Connecting a mobile phone to the computer to monitor TikTok, Snapchat and other social media can make such surveillance easier.

OSINT and SOCMINT can lead to useful information for law enforcement: domain name, screening social media and stand-alone websites. Who is the registrant? A video capture software to show the behaviour of the website. Some tools allow to generate an automatic GIF. There is some specialised software for investigators, to collect all the necessary info.
– Private investigator of IP crimes

- Constantly monitoring and analysing websites, including e-commerce platforms and other online marketplaces, to identify listings, product descriptions, or images that may indicate infringements. This can include monitoring online forums, communities, and boards where infringing activities are likely to be discussed. Domain name registrations and changes can also be monitored to identify suspicious behaviour. Useful information for investigating authorities can be obtained through OSINT by examining the domain name and screening social media and standalone websites to identify the registrant. The source code of the website can also be useful in connecting investigations or investigative targets. This source code can show interesting connections to other websites and help in establishing the identities of those running the website or even the owner. A VPN and/or a 'cold computer' – a standalone computer connected to a different server that cannot be traced back to the IP owner – can be used to visit websites and avoid detection.

IP Crime Case Example
A criminal referral presented by the IP owners' representatives was the result of monitoring activities conducted on the infringer's app. The criminal referral detailed the history and progressive diffusion of the infringer's app worldwide and in the national market as well as presenting information on the whole service, especially on the use of the BitTorrent protocol on which the infringer's app was based as well as on the specificities of the app itself. The criminal referral also included information on the main websites from which it was possible to download the infringer's app while a core part of the referral consisted of extensively documented references to the growth of the infringer's app service globally and in the national market, which represented a real threat to the legitimate industry. In particular, the IP owners' representatives provided evidence on the popularity and growth of the infringer's service, its functionalities and user-friendly layout as well as on the recent content available.

IP Crime Case Example
One productive tactic that the IP owner used was to subscribe to the illegal television service as a customer. This approach enabled the IP owner to gain insights into the infringer's modus operandi and network activities, which would later provide valuable evidence in court. Once the IP owner had obtained the needed equipment and a username the IP owner was able to access the infringer's system and see the internet addresses to which their equipment connected. By placing a device between the equipment used to facilitate the copyright infringement and the internet, the IP owner's experts could observe the network traffic. The experts proceeded by selecting channels from the infringer's system and observing the address from which the equipment received data streams. The IP owner could see that the equipment received electronic codes for decoding the satellite broadcasts (illegal card-sharing) from the infringer's website and the IP owner also identified the specific IP address with which it was associated. The IP owner was similarly able to identify from which network addresses the equipment was receiving illegal streams; in this way, two additional internet (DNS) addresses were implicated in the illicit operation.

- Searching and analysing images and videos. IP owners can use readily available reverse image search tools to identify instances of unauthorised use of copyright-protected images or trade mark-protected logos. This can help uncover instances where infringing images or videos are being used on websites, social media, or other online platforms.

- Requesting services from investigators or specialised OSINT professionals who are experienced in conducting online investigations for IP infringements. They can employ advanced OSINT techniques, tools, and methodologies to gather and analyse information effectively.

- Constantly monitoring customer feedback, reviews, or complaints on online platforms to identify instances of IP infringement. Customers often report counterfeit or infringing products, providing valuable leads for further investigation.

- Constantly monitoring and analysing any of the available financial information. This can include following invoices, bank transfers, and cryptocurrency transactions.

- Analysing the source code of a website to link investigations for advertising or property codes. This can help not only to identify the owner of the website, but also connect multiple websites to the same infringer. These connections can be found by looking at various data points, for example, using the information obtained from images to find a connection with other data, such as accounts or websites.

- Connecting the dots between the information found by using OSINT and other elements found during the analysis, including aspects such as the online behaviour of the IP criminal and patterns in the criminal's activities.

When conducting OSINT investigations, it is very important to preserve the evidence obtained using OSINT tools before the relevant content is eliminated or modified due to the changing and ephemeral nature of the online environment. This can be achieved through various strategies, including by taking screenshots and saving them with the source and date accessed, using video capture software to show the behaviour of the website, or recording and transcribing online chats and conversations.

II.A.3.e Public registry information

IP criminals frequently form entities to conduct their business – sometimes to hide their individual identities through an elaborate network of shell companies or entities. These entities may be engaged in both legitimate and illegitimate business enterprises, and the IP criminals operating these entities must often register identifying information in the public registry where such entities are registered and created. Some countries make the registries available online; others can only be reviewed by the public in person. In either case, they are available to the public.

Like any other member of the public, IP owners can access these public registries, which can provide a plethora of valuable information in identifying the suspected IP criminals behind these entities. Such information can include the names, telephone numbers and email address, and street addresses of corporate officers, as well as the addresses of the entities themselves. All this evidence can be used as evidence attributing certain IP crimes to specific individuals or entities.

II.A.4 Information about IP owner loss

Calculating how an IP crime causes loss to an IP owner can be a complex process that may not always be possible. For this reason, IP owners often rely on statutory damages in civil IP infringement cases. Nevertheless, where an IP owner can make a reasonable calculation of loss, it can be helpful to a criminal referral. Calculating IP owner loss involves assessing the extent of the infringement and the financial losses incurred as a direct result of this

infringement. Several general steps that can be followed to obtain the information about the IP owner's loss, including the following:

- Gathering whatever relevant evidence may be available in connection with the IP crime (*e.g.*, sales records, contracts, and documentation that establishing the extent and impact of the infringement),
- Determining the scope of the infringement (*e.g.*, identifying specific products or services that were subject to infringement and calculating the number of units sold),
- Establishing the revenue per unit (*i.e.*, the average revenue generated per unit of the legitimate product or service), and
- Calculating the revenue lost due to the infringement (*i.e.*, by multiplying the number of infringing units by the revenue per unit).

In some cases, if a competition clause exists in an agreement with another entity, IP owners cannot disclose information on the specific values of those agreements. Therefore, they often rely on academic studies, or they need to search for calculations that are accepted publicly.

As presented more fully below in the section on how to prepare a criminal referral, calculating IP owner loss can help persuade investigating authorities to accept an IP owner's criminal referral for investigation. In addition, this loss calculation can support a restitution claim that the court can consider when awarding damages to the IP owner as the victim of an IP crime. These may also include statutory or punitive damages, depending on the laws in the specific jurisdiction. Another loss calculation that an IP owner can make is the cost incurred to mitigate the damages caused by an IP crime. Moreover, the infringer's efforts to remedy the loss caused by the infringer's conduct can sometimes be considered to limit an IP owner's loss calculation.

Furthermore, it is relevant to include information that could prove causation, such as by demonstrating a causal link between the IP crime and the financial losses suffered. This may involve, for example, showing that the infringement directly resulted in the decline of sales or market share, leading to financial harm. Establishing this link will not always be easy or even possible for every IP crime case. Nevertheless, where such evidence is available, an established causal link between the IP crime and the financial losses suffered as a result strengthens an IP owner's claim of loss.

IP owners can tailor the formula to calculate their loss, especially to fit any requirements of local investigating authorities. Sometimes IP owners provide an estimate that is based on some clear metric, such as the number of goods seized in a given time period.

II.A.5 Information about infringer gain

Securing information about how much money the infringer has made is not as easy for IP owners as it is for investigating authorities. Some IP owners have retained law firms to facilitate the identification of an infringer's assets while others have had success in seeking the information from intermediaries such as the host of an infringer's website or the provider of online advertising to the website.

Some IP owners estimate infringer gain based on publicly available information about website visits and making comparisons with other websites and estimates of how likely it is customers will pay to obtain, download, or stream an infringing item. Estimates based on information found on the infringer's own social media accounts, such as how many followers or posts they have, or how much website traffic there is, can also assist in calculating how much the infringer gained.

Occasionally, IP owners can obtain information about an infringer's gain from the IP criminal's competitors who are cooperating with the investigation. Some IP criminals may even advertise or boast about how much money they have made from IP crime. Although these boasts can be mere puffery, they are sometimes accurate descriptions of an infringer's gain.

In any event, information about infringer gain can be closely related to establishing that counterfeiting or piracy crimes occurred – particularly on a commercial scale (*i.e.*, on the same scale as typical commercial activity), which is often a necessary element to an IP crime.

II.A.6 Third-party or customer loss

Although IP owners are often not in the best position to accurately measure how much loss a third party or customer suffered as a result of an IP crime, securing at least some information on such losses can still be helpful to highlight the impact of the crime.

For example, some counterfeiters successfully deceive almost every downstream party in the supply chain – including the wholesaler, the retailer, and the customer. When the counterfeit product is discovered, every one of these third parties has suffered a loss as they have each sold a counterfeit good thinking that it was authentic. Wholesalers and retailers may suffer measurable losses in the forms of refunds, and customers suffer calculable losses in how much they paid for a counterfeit good they believed was authentic. Customers may suffer additional measurable losses, such as the cost to replace the counterfeit good, medical costs when harmed by a counterfeit good, lost wages, and other consequential losses.

IP Crime Case Example
A defendant imported and sold several counterfeit transmission products as originals, mainly ball bearings and roller bearings. The defendant did so taking advantage of the fact that he had been an official distributor of a famous brand for many years. Among his customers, there were several companies active in industrial production. One of them, producing stainless wire rods and stainless wires, had purchased several transmission products from the defendant over the years to be used in one of its steel mills. However, the customer experienced several quality and functional issues with a batch of deep groove ball bearings purchased from the defendant. Under normal conditions of use, the bearings produced unusual vibrations and noise, forcing the customer to remove them from their machines, resulting in disruption to the work of the steel mill. The purchasing manager of the customer exchanged several emails with the defendant to report the product malfunction and have the bearings replaced. Unable to obtain a satisfactory solution, he turned directly to the producer (IP owner) and its product verification department, which confirmed that the ball bearings in question were counterfeit.

II.B Guidelines specific to copyright cases

Copyright validity. As noted above, copyrighted works are original expression fixed in a tangible medium. Thus, part of the copyright owner's preliminary investigation would include gathering evidence establishing that the copyrighted works relevant to the investigation are valid copyrights reflecting expression original to the copyright owner. If the owner of the copyright is not also its author, then the copyright owner should also gather evidence showing the valid assignment from the author to the current copyright owner of ownership rights to the copyrighted work.

Because most Berne Convention parties, including countries in Europe, do not offer the opportunity to register copyrighted works, copyright owners can identify witnesses during a preliminary investigation who could testify that a work of expression is original and is subject to copyright protection. If the copyright owner happens to have registered a work in a country where one can register copyrighted works – like the United States – then a copyright owner can use a certified copy of the copyright registration from that country to simplify establishing the validity of the copyrighted work that an infringer is alleged to have infringed. Although such a registration may not be dispositive evidence of a copyright's validity outside the country where the work was registered, it can be introduced as persuasive evidence, or even *prima facie* evidence, of the work's validity.

Test purchases of infringing copies or infringing streams of copyrighted works. Today, most copyright crimes occur online in the form of digital piracy. As a result, copyright owners must rely on technology more than ever as part of their preliminary investigation.

For example, in the context of a test download or test stream, copyright owners can take screen shots to document the offer of an infringing download or stream and the completion of the transaction – as well as every step in between. Copyright owners may also use specialised software to make a video recording every step the copyright owner took online when making the test purchase or download.

IP Crime Case Example
The visual analysis of a website confirmed the suspicious nature of its operations, and the IP owner's investigators decided to deepen their investigations and conduct a test purchase. The findings from the test purchase were another key component of the criminal referral since they demonstrated the website's illegal activity. To make the test purchase, the investigators contacted the website's customer service department through the channels given on the website. The website offered a 3-day voucher giving full access to the content of the offer before deciding to purchase a subscription. Using this voucher, investigators started collecting information through real-time analysis and testing of the channels, allowing the investigators to determine that all the channels were functioning without problems at a high level of quality and without buffering or chopping. Snapshots were taken and included in the criminal referral, including an analysis of the servers from which the channels were streamed; this was conducted via the browser's built-in functionality. The investigators purchased a subscription for the IP-infringing service via email. The investigator also ordered a set-top box, in order to conduct a complete analysis of all the features offered by the infringers' service.

IP Crime Case Example
Following the initial examination of some infringing websites, the investigators began the process of making a test purchase of the advertised infringing service via the infringing website. The investigators took screenshots of the infringing websites and the related Facebook pages for the websites. The investigators then contacted the IP criminals behind the website to make the test purchase of the advertised service. The device facilitating the infringing service was purchased, and the infringers provided an invoice describing it as a 'satellite system'. It was delivered and subsequently forensically analysed.

Copyright owners can use tools to track every IP address the copyright infringer forced the test purchaser to pass through before obtaining the infringing download or stream. This is particularly helpful, as every unique IP address visited before downloading an infringing item from a cyberlocker (or streaming an infringing item from a server) represents an independent

repository of helpful evidence. Each IP address visited represents a potential venue where a criminal case could be referred.

In cases involving downloads of infringing copies, copyright owners can document what technology was used to effectuate the distribution online: file transfer protocol (FTP), BitTorrent, etc., as well as the country in which each domain name is registered.

Finally, copyright owners can gather evidence of whether what an infringer is offering is, in fact, the infringing copy or stream that it purports to be. Thus, the test purchase process for copyright owners includes a 'test' of whether, for instance, an infringing song, movie, or video game is in fact an infringing copy of a copyright work. Copyright owners can make this determination by playing a sample of the infringing song, movie, or video game downloaded, or by streaming the infringing public performance. As with the test download or stream, copyright owners can document that a particular infringing copy 'played' properly using a video camera or special video software. When there is restricted access to Internet-based content based on the user's geographical location (known as geo-blocking), a virtual private network (VPN) can be used. Later, it can be highlighted in the criminal referral that the content is available only from a specific territory.

Attribution and identification of copyright infringers. Online piracy groups often compete with each other to earn the 'best' reputation for pirating particular types of copyrighted content. Some groups claim to have the highest-quality pirated works with the fewest glitches, other groups claim to have the most copyright infringing content, and others claim to be the first to 'crack' and distribute infringing copies of copyrighted works that use technological protection measures. Such piracy groups will sometimes include file extensions to demonstrate that they are the group that pirated a particular work. Others will include a .nfo file identifying the piracy group as the one that distributed a particular infringing copy. Copyright owners can try to obtain and track this type of information as part of their preliminary investigation.

Retail value of a copyrighted work. Article 61 of TRIPS requires signatory countries to impose criminal penalties on those who commit wilful piracy of copyrighted works on a commercial scale. Some countries impose higher maximum prison sentences when such copyright crimes also involve a commercial purpose, such as private financial gain. For this reason, copyright owners can find it helpful to gather evidence of the retail value of the copyrighted works at issue as part of their preliminary investigation.

Copyright owners sometimes sell the same copyrighted works at different prices, depending on where the work is sold. Prices may vary by country, by region, or even by city. Thus, copyright owners can gather the retail price information in conjunction with identifying the market where the infringement takes place. If a work is widely sold throughout the world, then copyright owners can limit their gathering of retail price data to those venues where the case may be referred for criminal investigation.

The calculation of the retail value of a pre-release work – such as a movie that is only showing in cinemas and not yet available to customers to purchase, download or stream legally – poses particular challenges. How a pre-release work should be valued can vary by the type of content as well as by the timing of the infringement. For example, a movie that is not yet available for viewing in cinemas may have more value than a movie that is already in theatres but not yet available for purchase, download, or streaming – even though both of these movies may be

deemed ‘pre-release’ as a matter of law. In the same vein, piracy of an upcoming music album one day before its release to the public may cause less harm than piracy of the same album six months prior to its release. Copyright owners can gather evidence of the cost of lost sales as a result of pre-release piracy as well as how much the copyright owner may charge for the pre-release work to others (*e.g.*, the price for a movie sold to a hotel chain or an airline) before it is released to customers.

Related crimes. Copyright crimes often occur alongside other crimes, and copyright owners may spot and gather evidence of these other crimes while gathering evidence of the copyright crime. For example, during a preliminary investigation, copyright owners sometimes discover evidence of computer hacking by an infringer to obtain access to a pre-release work. Copyright owners may uncover evidence that the distribution or streaming of infringing copies of their works also includes the distribution of malware that could facilitate a ransomware attack, unauthorised access to a computer network, or wire fraud. In tracking the financial information associated with a test download or test stream, copyright owners may even come across various entities through which the infringer is laundering money. In addition, many digital copyrighted works are protected by technological protection measures. Wilfully circumventing, or facilitating the circumvention of, such measures for commercial purposes can constitute a separate crime that often occurs alongside a copyright crime. Copyright owners can gather evidence of this circumvention crime (and the facilitation of this crime) as well.

II.C Guidelines specific to trade mark cases

Trade mark-specific evidence. Trade mark owners register their marks in national and regional trade mark or IP offices. During a preliminary investigation, trade mark owners can obtain certified copies of each registered trade mark that has been counterfeited to establish their validity more easily than copyright or trade secret owners can. Such evidence can also be useful to combat cybersquatting or typosquatting fraud, in which the victims may be the website users in addition to the trade mark owner whose word mark was used to create a domain name without the trade mark owner’s permission.

Trade mark owners should take care, however, to obtain certified copies of the relevant trade marks for the same class of goods on which the defendant has used the counterfeit mark. For example, during the preliminary investigation of the use of counterfeit marks on handbags, the trade mark owner would obtain a certified copy of the registration for the trade mark's use on the class of goods that include leather goods (like handbags) rather than the registration for the class of goods that includes clothing. Trade mark owners are in the best position to know their own trade marks, and they can gather the certified copies of the correct trade mark registrations more efficiently than investigating authorities can.

A certified copy of a trade mark registration may create a rebuttable presumption of its validity, but it does not establish that the trade mark was in use when the criminal counterfeiting conduct occurred. To establish the timing of the trade mark owner's use of a mark, trade mark owners can identify and gather evidence showing, or witnesses who can testify, that a trade mark owner was in fact using the trade mark at the time of the counterfeiting offence.

Counterfeit labels and packaging. Some counterfeiters will traffic in labels bearing counterfeit marks that are unattached and separate from the goods to which the counterfeiter will ultimately affix them. When trade mark owners conduct a preliminary investigation of such cases, trade mark owners can identify and gather evidence not only of the labels bearing counterfeit marks but also of the equipment that the counterfeiters may be using to attach such labels and otherwise facilitate the counterfeiting conduct.

In addition, trade mark owners can establish a verification procedure to determine whether labels and packaging are counterfeit. Brand owners change product packaging from time to time, and tracking those changes is the first step in a verification procedure. This step will allow the IP owner to determine whether a product using old packaging at the time of the IP crime is in fact using counterfeit versions of the authentic "old" packaging. Brand owners can also track when old packaging is no longer in use such that even high-quality counterfeits of old packaging are exposed as counterfeit simply because such packaging is no longer in use.

Related crimes. As with copyright crimes, criminal trade mark counterfeiting often occurs alongside other crimes, and trade mark owners may spot and gather evidence of these other crimes in the course of gathering evidence of the counterfeiting crime. For example, during a preliminary investigation, trade mark owners may discover evidence of smuggling whereby counterfeit goods are mixed with, or hidden within, generic or otherwise legal goods. Counterfeiters may engage in mail or wire fraud when they traffic in counterfeit goods, and trade mark owners can gather evidence of these crimes too. In tracking the financial information associated with a test purchase of a counterfeit good, trade mark owners may even come across various entities that the infringer is using to launder money and can gather such evidence as well.

II.D Guidelines specific to trade secret cases

Evidence related to the trade secret. During a preliminary investigation, trade secret owners can gather information that generally describes the trade secret without revealing it. Such evidence can include the type of trade secret (*e.g.*, source code, chemical formula, technological methods, or processes, etc.) and whether the information has ever been published in a trade journal or registered as a patent.

Trade secret valuation. Trade secret owners can use a preliminary investigation to estimate a trade secret's value. Many methods can be used to estimate a trade secret's value: the cost to develop the trade secret, the cost to acquire the trade secret, the price a reasonable purchaser would pay for the trade secret, or even the costs imposed on the trade secret owner as a result of the theft of the trade secret.

Reasonable measures used to protect the trade secret. A preliminary investigation can include gathering evidence establishing what type of reasonable measures the trade secret owner took to protect a trade secret. These measures often take three forms: physical protection, electronic protection, and company policies and practices designed to protect trade secrets.

- *Physical protection measures* protecting locations housing trade secrets can include:
  - Physical barriers to entry into a facility housing the trade secret
  - Guards limiting entry into buildings or rooms housing trade secrets

  - Requiring that visitors be escorted at all times
  - Locks on doors, cabinets or drawers or other storage facilities
  - Alarms on doors
  - Video surveillance
  - Requiring a key card for entry
  - Logging access to the location where the trade secret is stored
  - Limiting which employees have access to a trade secret through the use of a key, key card, or biometric information

- *Electronic protection measures* protecting trade secrets can include:
  - Requiring passwords
  - Using firewalls and virtual private networks
  - Using secured laptops that preclude the use of external devices such as thumb drives
  - Encrypting the trade secret data
  - Precluding remote access
  - Logging each attempted electronic access to a trade secret

- *Company policies and practices* designed to protect trade secrets can include:
  - Requiring employees and potential business partners to sign non-disclosure agreements
  - Distributing policies regarding the handling of trade secrets to all employees
  - Training employees on the proper handling of trade secrets
  - Imposing a policy limiting the disclosure of trade secrets only to those employees who 'need to know'
  - Marking trade secret materials as 'proprietary,' 'confidential,' or 'trade secret'
  - Conducting exit interviews with departing employees that include
  - emphasising the trade secret owner's confidentiality policy
  - obtaining all company storage devices
  - confirming the return of all proprietary or confidential information
  - emphasising any non-disclosure agreements, training, and policies related to trade secrets

Related crimes. Trade secret theft often occurs alongside other crimes, and trade secret owners can gather evidence of these other crimes in the course of gathering evidence of the trade secret theft. For example, many trade secrets take the form of source code, which can also constitute original expression protected by copyright law. Thus, during the preliminary investigation of the theft of source code establishing a trade secret, a trade secret owner may also consider gathering evidence consistent with the above guidelines specific to a copyright crime. In addition, trade secret owners sometimes discover evidence of computer hacking by an intruder seeking to obtain access to a trade secret stored online. Moreover, trade secret owners may uncover evidence that a thief engaged in some form of fraud through social engineering to obtain unauthorised access to the trade secret. A thief may have stolen the identity or credentials of an employee to gain unauthorised access to a trade secret. Trade secret theft is sometimes accompanied by ransomware whereby the thief encrypts servers storing the trade secret, and then refuses to provide the key granting access to the trade secret until the owner pays a ransom.

III Preparing a criminal referral

III.A Generally applicable guidelines

III.A.1 Factors to consider in deciding whether to make a criminal referral

Factors to consider when deciding whether to make a criminal referral

Upon discovering an infringement of their IP, IP owners must decide what action, if any, they will take to for enforcement. Among the most common choices are civil enforcement, private criminal enforcement, or a criminal referral to investigating authorities. In deciding whether to pursue a criminal referral, IP owners may consider a variety of factors, including the following:

Commercial scale. Although an IP owner could theoretically refer every infringement of its IP to investigating authorities, it is not realistic to expect an investigative body with limited resources to successfully prosecute every conceivable IP crime. For this reason, IP owners consider the scale of the infringement in deciding whether to make a criminal referral and investigating authorities often do likewise in deciding whether to open an IP crime investigation. Cases involving the largest commercial scale – such as online piracy cases involving hundreds of thousands of infringing items, or a counterfeit goods case involving tens of thousands of counterfeit goods – are often the subject of criminal referrals. A large commercial scale often goes hand-in-hand with large illicit proceeds for the IP criminal – another factor that investigating authorities consider in deciding whether to accept a criminal referral.

Focus on big cases in a criminal referral. Look for who is behind the large-scale crime, how big the threat is, and the website traffic. Sometimes we are looking for an actor that uses a lot of different domains, and we can prove a connection between different actors. We often have a history of sending takedown notices – the IP criminals are already well aware of our attempts to take them down.
– IP owner

What constitutes the 'right' amount of commercial scale can depend on the industry, the type of IP involved, and the presence of other factors for consideration as set forth below. For example, theft of a single trade secret may merit a criminal referral – even though it is a scale of one – if the impact of the theft of a company's most important trade secret could destroy the trade secret owner's business.

Complexity. IP crime cases can be among the most complex cases to investigate. Such crimes are often perpetrated by sophisticated actors using cutting edge technology and who take advantage of resources in multiple jurisdictions – making them harder for one investigating authority to pursue. IP crime cases can also involve criminal groups using dozens of shell corporations that make it difficult, if not impossible, for the average IP owner to investigate. Although IP owners may be more familiar with the IP that they regularly enforce than are investigating authorities, IP owners do not have as many tools to investigate a complicated IP crime case. For this reason, IP owners often consider the complexity of the case as a factor that weighs heavily in favour of making a criminal referral.

Impact. When the impact of a particular IP crime on IP owners is high, IP owners can both rely on this factor in deciding whether to make a criminal referral and can emphasise this factor in the referral. What constitutes a high impact case will depend on the IP owner. Moreover, the largest-scale case may not necessarily make for the highest impact case referral. For instance, online piracy of a pre-release version of an upcoming blockbuster movie may have a greater impact on a motion picture company than an illegal cyberlocker hosting hundreds of copies of pirated movies. The motion picture company may prioritise referring the pre-release piracy case to investigating authorities. Similarly, small-scale counterfeiting of a widely sold perfume may have a greater impact on the brand's reputation and customer safety than counterfeiting of the same brand owner's handbags. Even for trade secret cases, theft of a customer list that arguably qualifies for trade secret protection may have less impact on the trade secret owner than the theft of the source code of that owner's best-selling software.

It is necessary to indicate a public interest in the referral. The referral needs to touch on the substance of the case -- what IP has been infringed and which goods are affected. For instance, the impact will vary when the goods involved are pharmaceuticals, software, or t-shirts.
– Outside counsel for IP owners

Health and safety. Some IP owners own IP that implicates health and safety. Protecting health and safety is a high priority for the public, investigating authorities, and IP owners alike. Accordingly, IP crime cases involving such threats weigh heavily in favour of criminal referral.

Organised crime. Although many IP crimes are committed by individuals, increasingly large-scale, high-impact IP crimes are committed by organised crime groups. Although IP owners frequently deal with individual IP criminals, IP owners are often ill-equipped to confront the various challenges posed by organised crime groups. Thus, when an organised crime group is responsible for the particular IP crime being considered for criminal referral, this is a factor that weighs heavily in favour of making a criminal referral.

Related crimes. As already noted, IP crimes like criminal copyright infringement, criminal trade mark counterfeiting, and trade secret theft are often accompanied by other serious crimes such as computer hacking, fraud, smuggling, and money laundering. The presence of such additional crimes increases the likelihood that investigating authorities will accept the criminal referral, especially if they place a higher priority on such other crimes. As a result, when an IP owner discovers that other serious crimes are occurring alongside an IP crime, the IP owner may consider this factor in favour of making a criminal referral.

High number of victims. In large-scale IP crimes, IP owners will often discover that they are not the only victims. Other IP owners, customers, and even governments can all be victims of an IP crime. The higher the number of victims, the more likely it is that investigating authorities will accept a criminal referral. Thus, the number of victims is a factor IP owners should consider when deciding whether to make a criminal referral.

Civil remedies are unavailing. Certain types of IP cases arise where civil remedies are simply unavailing, making such cases strong candidates for criminal referral. For example, even though an IP owner can successfully pursue a street vendor selling copyright infringing or counterfeit goods for civil monetary damages and injunctive relief, the vendor may be unable to pay the damages and unwilling to adhere to an injunction. The IP owner can continue suing the street vendor for further damages or court orders, but the vendor will remain undeterred. As such, the only way to deter the vendor may be through criminal enforcement. Indeed, local police frequently pursue low-level IP criminals for this very reason. The same challenge may exist when pursuing civil remedies against a wealthy infringer. For instance, a factory owner producing vast amounts of counterfeit goods may be able to absorb the loss of occasional shipments seized by customs and afford to pay civil judgements, even those amounting to millions of dollars – as the cost of doing business. The only way to deter such a large-scale IP crime operation may be through a criminal referral.

Cost vs. control. From an IP owner's perspective, oursuing a civil IP case can be very expensive, even for larger IP owners. In contrast, preparing a criminal referral – while not cost-free – often requires fewer investigative resources than preparing a civil complaint, and the government bears the costs of further investigation and litigation if the criminal referral is accepted. At the same time, IP owners have little control over an IP case once a criminal referral is accepted. Sometimes it is important to the IP owner that it be in control of the IP case – the IP owner's case may be time sensitive and cannot wait for a criminal process that sometimes will be too slow. For this reason, IP owners must balance the cost savings benefits that come with a successful referral against the lack of control that typically occurs.

Venue. The venues where an IP crime occurs may limit where a criminal referral can be made. IP owners may perceive that some jurisdictions are less likely to enforce IP criminal laws, and that may be a factor weighing against a criminal referral. On the other hand, IP owners may have developed a good relationship with certain investigating authorities' offices, and that may be a factor weighing in favour of a criminal referral.

III.A.2 Changes to an IP owner's behaviour after deciding to make a criminal referral

The changes in an IP owner's behaviour after making a criminal referral may depend on the targets of the IP investigation. An IP owner may not wish to send a cease-and-desist letter or a takedown notice in pursuit of a criminal referral – even though the IP owner might otherwise do so in the normal course of confronting infringers – because the IP owner may not want to 'tip-off' the targets that the IP owner is investigating them. Similarly, investigating authorities may advise IP owners that they are considering a criminal investigation and ask the referring IP owner not to take any action that may alert the targets that they are under scrutiny.

On the other hand, the targets of the IP investigation may very well be the subject of a criminal referral precisely because the targets have already received dozens of cease-and-desist letters or takedown notices and have ignored them. In this situation, an IP owner's behaviour may remain unchanged. In fact, the IP owner may not want to change its behaviour in order to further establish the target's impunity – evidence that investigating authorities and prosecutors can use to further establish the target's wilful conduct.

III.A.3 Choosing which details to emphasise

Most criminal referral packages will include an executive summary of the case being referred, identify the IP owner and other victims of the IP crime, and identify the type of IP that is involved. Beyond these necessary elements, it is important to consider which details to emphasise. Including every conceivable detail could make the criminal referral package so long that no one reads it and, more importantly, it may not receive the priority from investigating authorities that it may deserve. At the same time, providing insufficient detail may suggest to investigating authorities that the IP owner has not made its own good faith effort to investigate the IP crime, perhaps leading investigating authorities to de-prioritise or even decline the referral. For this reason, IP owners often offer to provide more complete details to investigating authorities at their request, but ensure that the initial referral package offers sufficient detail to answer the following critical questions:

What is the IP crime involved? It is important to identify what IP crime is involved and specify the law(s) that the IP owner believes the target of the investigation has violated. Identifying the relevant laws will immediately alert the recipient of the referral to the elements of the IP crime(s) that they would have to investigate. Along the same lines, the referral should include a brief summary of the facts discovered during the preliminary investigation in sufficient detail so that they may be organised according to each element of the IP crimes identified. For instance, the referral package should provide a summary of the evidence of wilfulness on the part of the suspected IP criminal and the scale of infringement, as these are necessary elements for almost every IP crime. Although an IP owner's preliminary investigation often will not have uncovered sufficient facts to prove each element beyond a reasonable doubt, understanding what evidence the IP owner has already discovered will help the recipient of the referral to determine which elements will require the most attention if the referral is accepted. This section of the criminal referral can also include a similar summary for any other crimes that the IP owner has identified that may be associated with the IP crimes involved.

Where did the IP crime occur? The referral package should provide sufficient detail to explain the connection between the IP crime and the venue where the IP owner is making the criminal referral. Not every detail needs be included – just enough to establish that the recipient of the referral has jurisdiction to investigate the case.

When did the IP crime occur? Although this detail may seem simple, when the IP crime occurred is dispositive for at least two reasons. First, the IP crime must have occurred within the statute of limitations; otherwise, the case cannot be investigated or prosecuted. Second, an older case may make obtaining evidence from third parties harder, especially electronic evidence that third-party intermediaries or service providers may not be required to preserve. Details regarding when the IP crime occurred are therefore essential to any criminal referral package. These details should also include, if known, the duration of the crime.

Who committed the IP crime? Although it is not always certain what the true identity of an IP criminal is after a preliminary investigation, attribution evidence as set forth above that an IP owner gathers can be very helpful to investigating authorities. At the same time, computer forensic evidence related to identifying an online IP criminal can be quite voluminous. Thus, IP owners may choose to provide a summary of the best forensic evidence found that identifies the suspected IP criminals. IP owners may then offer an external drive or thumb drive that includes the forensic details that the recipient of the referral can choose to accept at that time or at a later date.

Why did the IP owner refer this particular IP case for criminal enforcement, and **why** investigating authorities should accept the referral? IP owners can consider providing sufficient details in the referral package to explain why they are making a criminal case referral. As noted above, there are many factors that may lead an IP owner to make a criminal referral, and it is not necessary to explain every factor considered. Instead, IP owners may choose to emphasise those factors that would also make the case more appealing to the recipient of the referral. For example, most investigating authorities prioritise investigating crimes involving a threat to the public, such as threats to health and safety or the involvement of organised crime. Similarly, recipients of referrals often prioritise cases involving multiple crimes or a high number of victims. Investigating authorities also may prioritise larger and more complex cases that have the potential for the greatest impact on a particular type of IP crime. In addition, large-scale IP crimes involving a high amount of potentially illicit proceeds can be a priority for investigating authorities too. Tailoring an explanation of why the IP owner made the referral to also answer the question of why investigating authorities should accept the referral can maximise the likelihood that the case referral will be accepted.

Beyond answering these basic questions, there are other details that an IP owner may wish to emphasise or offer, depending on the type of case being referred. IP owners often hire attorneys in the country where the referral is being made to help choose which facts to emphasise. Some additional details that IP owners may emphasise include the following:

- what is the public interest, and how have customers and other third parties been impacted; including customer complaints can help demonstrate the public interest
- what civil actions the IP owner has already attempted
- whether the IP owner has made the same criminal referral to other investigating authorities
- what test purchases, downloads, or streams the IP owner may have made and how were they documented
- what information, if any, is there about the loss to the IP owner
- what information, if any, is there about the amount of money the infringer has gained
- what other cases are out there involving the same suspected IP criminals as the IP owners often know how cases involving the same IP criminals are interconnected better than the recipient of the referral

Most important, it is key for IP owners to let investigating authorities know in the referral package and in any related meetings that the IP owner will be available to assist at any time and provide the IP owner's best contact information to investigating authorities as part of the referral.

III.A.4 Overcoming thresholds

In many countries, investigating authorities have discretion to decide which criminal cases they will investigate. In exercising their discretion, investigating authorities may impose informal, unwritten thresholds that must be met before they will accept a criminal referral. For example, a particular law enforcement office may only accept cases above a certain scale of

infringement, or with a potential value above a certain amount. These offices may use such thresholds to ensure that they are devoting their limited resources to investigating only the most impactful cases.

Thresholds may vary from one law enforcement office to the next. For this reason, IP owners considering making a criminal referral may find it helpful to work with a local attorney or trade association with an established relationship with the law enforcement office to which the IP owner intends to refer the case to determine what thresholds IP owners may face there. IP owners may discover that they are not always able to meet a particular threshold based on scale or monetary value for every criminal referral.

Fortunately, thresholds are sometimes flexible, meaning that there may be ways in which IP owners can overcome them. In these instances, IP owners may wish to revert to the above-referenced factors that they considered in making the criminal referral to see how they may overcome the threshold – typically by emphasising the significance or impact of the particular criminal referral to a particular industry or to the public.

Usually there has to be an impact to the public to overcome a threshold.
– IP owner

For example, if a law enforcement office's threshold for accepting a criminal trade mark counterfeiting referral is a case involving more than 100,000 counterfeit goods and the IP owner's case only involves 20,000 counterfeit goods, then the IP owner may consider emphasising how this particular case impacts the public. Perhaps the case involves counterfeit pharmaceuticals that would impact the public's health and safety. Or perhaps the case involves counterfeit luxury goods being manufactured by immigrants who organised crime groups have illegally trafficked and forced to labour in sweatshop conditions. In some cases, it is possible to provide additional evidence supporting the allegation that the identified infringer may lead to another infringer who is a more serious target. Emphasising how investigating and prosecuting a case would clearly and directly impact the public is one of the best ways to overcome thresholds.

Small brands may have a particularly difficult time overcoming scale and monetary value thresholds. One strategy they can use is to reach out to trade associations. Trade associations often collect information about websites or marketplaces where IP infringements are impacting many of their members and can help member IP owners identify others that are in similar situations. If multiple IP owners suffer harm due to the same IP criminal actors (*e.g.*, the same website is infringing the copyrights or trade marks of multiple IP owners), then these IP owners may wish to present a criminal referral collectively. This is another strategy to overcome thresholds.

Another strategy would be to present the criminal referral to a different law enforcement office. Law enforcement offices responsible for bigger cities may have higher thresholds than those in smaller cities. Local attorneys can often advise IP owners on the thresholds of the respective

local law enforcement office. Note that the IP owner would still have to establish venue in all instances.

III.A.5 Understand the recipient of the referral

IP owners can consider the relative experience of the recipient of the referral with IP crime investigations. Some jurisdictions have specialised units of IP investigators and prosecutors who are quite familiar with the enforcement of criminal IP laws. However, most jurisdictions do not have such specialised units.

Although some IP owners have a unified standard approach to presenting criminal referrals, IP owners can consider tailoring their criminal referral to the particular recipient of the referral.

Normally we have a standard package, if we constantly work with the investigating authority in a single country, we will adjust some elements to their feedback.
– IP owner

For instance, when referring a criminal IP case to a law enforcement office with little or no experience investigating IP crimes, the IP owner may consider including a section in the criminal referral that explains which IP criminal laws apply and how they can be enforced. IP owners can even use wording in the referral that prosecutors and investigators can use in their own submissions. IP owners can even copy wording from the laws into their referrals that investigators and prosecutors can later copy and paste into a search warrant or indictment. Some law enforcement offices may even appreciate a pedagogic approach that saves them the time of learning the law themselves.

In some jurisdictions, it is even considered appropriate for the IP owner to include a draft indictment in the referral package. Some IP owners may deem it appropriate to offer investigative suggestions, such as identifying particular servers or devices to search.

Some IP owners have used a strategy of offering training to local law enforcement authorities where they may file a criminal referral so that office would be better prepared when the IP owner ultimately submits a criminal referral.

The golden rule is to make the job as easy as possible for investigating authorities.

III.A.6 Presenting and explaining the IP laws (including legislative framework) and issues involved

Once all the facts have been presented, the criminal referral typically includes a legal assessment. As stated above, IP owners often find it helpful to include a description of the legislative framework that authorised the recipient of the referral to investigate a violation of the particular IP law at issue in the referral. Some IP owners include this legislative framework

in every criminal referral, whereas others will only include it when the recipient of the referral lacks experience investigating the IP crime at issue in the referral.

As discussed more specifically below, IP owners can use the referral as an opportunity to explain the type of IP involved and the scope of its protection. IP owners can highlight areas where the law is clear and where it might be ambiguous, and even suggest ways in which those ambiguities can be resolved with the evidence included in the referral. Furthermore, as already noted, IP owners can organise the evidence that they have gathered according to the elements of the IP criminal law at issue. Organising the criminal referral in this manner allows the IP owner to highlight those areas where more investigation is needed, perhaps because certain relevant evidence is beyond the reach of an IP owner and can only be obtained by investigating authorities. Investigating authorities, in turn, can use this information to prioritise their investigation.

III.B Guidelines specific to copyright cases

Copyright owners can consider including all the specific information that they gathered as set forth and discussed in II.B. Beyond these items, copyright owners sometimes face unique challenges when preparing a criminal referral. Criminal copyright infringement cases rarely implicate health and safety, and often they do not involve criminal motivated by a commercial purpose. For example, certain criminal groups operating online, such as some ‘warez’ groups, engage in large-scale copyright crime online for the purpose of having the reputation for being the first to ‘crack,’ reproduce, and distribute infringing copies of the latest hit song, blockbuster movie, or cutting-edge video game. Although these online copyright criminals are not financially motivated, they can cause enormous harm to the copyright owners victimised by such piracy.

Although commercial purpose is not a necessary element of a copyright crime under Article 61 of TRIPS, investigating authorities are often far more likely to accept a criminal referral where there is a commercial purpose. How, then, can copyright owners overcome a commercial purpose threshold? One strategy copyright owners can use is to limit criminal referrals to the most egregious actors causing the most harm to the greatest number of copyright owners – such as the cyberlocker distributing the greatest number of infringing copies of pre-release works for free, or the streaming site broadcasting the most live sports events in real time for free. This approach allows the copyright owner to show that they are only asking investigating authorities to investigate those online pirates inflicting the greatest harm to a particular copyright industry (such as music, movies, or video games) or sometimes even to more than one industry.

This strategy also has the benefit of overcoming another unique challenged faced by copyright owners – the so-called ‘whack-a-mole’ problem. Some law enforcement offices decline copyright criminal referrals on the basis that shutting down one website will simply lead to a new one taking its place. However, the online piracy groups competing for reputation are not as easily replaced; customers of their infringing copies and streams know them by name, and they download and stream their content precisely because of these groups’ reputations. Thus, IP owners can persuasively argue that, by taking down these highest impact online piracy

groups, they can disrupt an entire ecosystem of piracy – not just a single website – that is not easily replaced.

Another strategy copyright owners can use in preparing a criminal referral is to present a referral that is unique – either in the type of content being pirated or in the technology that the online pirates are using. Some law enforcement offices – particularly those that include specialised IP units – seek to investigate 'first of its kind' cases or cases with unusual technological complexity.

To increase the likelihood that investigating authorities will accept their referrals, copyright owners can consider emphasising other crimes that may also have occurred that investigating authorities may prioritise over copyright crimes. For instance, computer hacking, and identity theft are often involved when a copyright criminal attempts to access a digital copy of a pre-release song, movie, or video game. Some online pirates facilitate fraud using malware in the advertising on their websites. Furthermore, many copyright criminals engage in money laundering with the proceeds of their copyright crimes. Highlighting related crimes that may be involved in the criminal referral can be a helpful strategy for copyright owners to follow.

As noted in the guidelines above related to what information copyright owners could gather for a criminal referral, copyright owners may wish to pay particular attention to including evidence regarding the validity of the copyrights at issue in the criminal referral. Unlike trade mark owners, copyright owners in Europe generally cannot rely on a registration in a national or regional IP office. Including information informing investigating authorities why the copyrights at issue are valid in the criminal referral can assure them that the issue of copyright validity is unlikely to arise.

Regarding test purchases, downloads and streams, copyright owners can consider placing particular emphasis in documenting how they gather some of the information referenced above in II.B. For example, copyright owners may not only consider taking screenshots as they make a test download or stream, but they may also wish to employ special video software to show every step they take online during the test purchase. Copyright owners may also want to use online tools to track the various IP addresses to which they are redirected from the public-facing site where a test purchase begins until they reach the ultimate site where the test download or stream occurs. Finally, in the case of downloads, copyright owners may also want to confirm that the infringing copy of the song, movie, video game or other content that was downloaded is in fact what it represents itself to be and operates as expected.

Finally, the fact that most copyright crimes today occur online means that copyright owners can consider highlighting the attribution and identification evidence they have collected regarding the copyright infringers. IP owners can include such information to alert investigating authorities to the suspected targets of the investigation and what, if any, further investigative steps they may need to take to identify any targets that the copyright owner was unable to identify.

III.C Guidelines specific to trade mark cases

Trade mark owners can consider including some or all of the information that owners may gather for a criminal referral referenced in II.C. Trade mark-specific evidence can be especially easy to include, and especially useful to investigating authorities. Identifying which trade mark registrations apply, providing evidence that the trade marks were 'in use' by the trade mark owner at the time of the counterfeiting offense, and establishing that the counterfeiter has used the mark on the same class of goods for which the trade mark is registered are all elements that trade mark owners can include, and investigating authorities will welcome seeing, in a criminal referral package to easily establish the validity of the trade marks.

If the case does not involve a counterfeiter's use of a mark identical to a registered trade mark but rather one that is substantially indistinguishable from the registered mark, then the trade mark owner may wish to include a description of what nominal differences may exist between the two marks. The trade mark owner may then wish to explain why the mark the counterfeiter used is still considered a counterfeit substantially indistinguishable mark and not merely a mark that is a colourable imitation of the registered trade mark.

Although Article 61 of TRIPS only requires signatories to impose criminal penalties where counterfeit marks are involved, some countries nonetheless also criminalise wilful trade mark infringement on a commercial scale when an infringer uses a mark that is merely a colourable imitation of the registered mark. In such jurisdictions, trade mark owners may wish include an explanation in their criminal referral explaining why the mark the infringer used is a colourable imitation of the registered trade mark likely to cause confusion among post-sale customers.

Trade mark owners can also provide helpful information on test purchases made in physical and online markets. For test purchases in physical markets, trade mark owners can include photographs of the counterfeit goods at a vendor stall that clearly show the use of the mark on a good in the market, as well as more detailed photographs of the goods upon purchase. They can also include photographs of the counterfeiters themselves as well as anything that might identify the counterfeiter such as a business card, a name tag, or even a car license or number plate (if the car clearly belongs to the counterfeiter). For online markets, as in the case of copyright owners, trade mark owners may wish to document the transaction with screen shots and online videos of the sites visited to complete the sale.

Trade mark owners may also wish to include details of tests conducted on both the product and any accompanying labels and documentation to establish that the product or the labels (or both) are not authentic. This can be particularly helpful in jurisdictions that independently criminalize trafficking in counterfeit labels designed to be used in connection with the same class of goods for which the mark is registered.

Trade mark owners may also wish to emphasise if counterfeiting their goods implicate the health and safety of the public. A broad array of counterfeit goods – such as counterfeit pharmaceuticals, perfume, automobile parts, and alcohol – can directly impact the public's health, and trade mark owners may wish to emphasise such facts in their criminal referral. As already noted, most law enforcement offices prioritise investigating cases where the public's health and safety are implicated.

Some jurisdictions impose higher maximum sentences or additional penalties when certain counterfeit goods are involved – such as counterfeit drugs, counterfeit pesticides, or counterfeit military equipment. Some jurisdictions also impose higher sentences where a counterfeiter placed customers at a higher risk of bodily harm or death. If there is evidence that counterfeiting has caused such higher risks or, unfortunately, already harmed customers, trade mark owners may wish to include these facts as well.

Finally, trade mark owners may wish to include evidence they have gathered regarding related crimes. Trade mark counterfeiters often engage in money laundering, smuggling, or mail or wire fraud when they traffic in counterfeit goods, and trade mark owners can include evidence of these related crimes in the criminal referral too. As already noted, investigating authorities tend to prioritise these related crimes over counterfeiting crimes, especially those counterfeiting crimes that may not implicate the public's health and safety. Thus, including evidence of these related crimes may increase the likelihood that investigating authorities will accept a trade mark owner's criminal referral.

III.D Guidelines specific to trade secret cases

Trade secret owners can consider including some or all of the information that owners could gather for a criminal referral referenced in II.D. Among the most important pieces of information to include is a description of the stolen trade secret sufficient to convince investigating authorities that a trade secret is, in fact, at issue. Unlike trade marks or patents, trade secrets are not registered and indeed cannot be publicly registered or else they will lose their trade secret status. Defendants accused of trade secret theft take advantage of the greater difficulty in establishing the validity of a trade secret by routinely challenging whether the property alleged to have been misappropriated qualifies as a trade secret. Thus, investigating authorities often scrutinises this aspect of a criminal referral in particular to determine how likely the government will succeed in rebutting this common defence. For this reason, trade secret owners often prioritise an explanation of why the stolen property at issue is a trade secret. This explanation typically includes a discussion of both the value of the trade secret and the reasonable measures that the trade secret owner has used to protect the trade secret.

Trade secret owners can also include in the referral package evidence of how the trade secret theft has harmed, or could harm, them. The evidence used to prove harm often hinges on an estimate of a trade secret's value. As already noted, many methods can be used to calculate such an estimate: the cost to develop the trade secret, the cost to acquire the trade secret, the price a reasonable purchaser would pay for the trade secret, or even the costs imposed on the trade secret owner as a result of the theft of the trade secret.

Trade secret owners typically include in the referral package a detailed description of the reasonable measures taken to protect the trade secret, as most jurisdiction consider this a necessary element of the definition of a trade secret. Thus, trade secret owners often include a description of the various physical measures, electronic measures, and company policies and practices designed to protect the trade secret at issue. Examples of such measures are set forth in II.D related to the gathering of evidence by trade secret owners.

As with other IP crimes, trade secret theft often occurs alongside other crimes, and trade secret owners can include evidence of these related crimes in their criminal referral. Computer hacking, extortion, cyber fraud, and other computer crimes are often associated with the theft of trade secrets in digital form. Including evidence of such other crimes in the trade secret criminal referral may increase the likelihood that investigating authorities will accept it.

IV Role of an IP owner during the criminal investigation

IV.A Generally applicable guidelines

Role of IP owner during the criminal investigation

1. Witness statements, affidavits and identification of goods

2. Assistance with searches and obtaining evidence

3. Chain of custody documentation

Once an investigating authority accepts an IP owner's criminal referral, then the criminal investigation begins. Although investigating authorities will now be in charge of the criminal IP investigation, the IP owner's role does not end here. In fact, IP owners remain active in IP criminal investigations because investigating authorities will routinely rely on their assistance throughout the investigation. Sometimes there will be regular but infrequent contact from investigating authorities; sometimes investigating authorities will be reaching out to IP owners on a daily basis. Either way, IP owners can consider designating one or more points of contact to be ready to support the criminal investigation.

IV.A.1 Witness statements on infringement, affidavits, and identification of IP-infringing goods

During an IP criminal investigation, investigating authorities will be assembling evidence that ultimately may be needed to prove the criminal case at trial. One of the most common features

of these investigations are the execution of search warrants – whether it is to search for evidence in the content of servers in a criminal copyright case, warehouses in a criminal trade mark counterfeiting case, or the personal devices of a defendant in a trade secret theft case. For this reason, IP owners can consider having a plan in advance of the criminal referral of what resources they will devote to supporting investigating authorities during the criminal investigation.

To establish the facts necessary to obtain a search warrant, investigating authorities may reach out to IP owners for statements or affidavits explaining (often in greater detail than in the referral) why particular items are infringing. Investigating authorities can rely on these statements and affidavits in their submission to a judicial authority for permission to execute a search warrant.

Although some IP owners have employees who can serve as fact and expert witnesses to identify infringing items and why they are infringing, other IP owners may use private investigators or outside experts to provide sworn statements. Often IP owners will provide extensive training to the private investigators or outside experts that they use. When IP owners rely on private investigators or outside experts to provide a statement or affidavit, they will typically explain what training they have had and what qualifies them to be private investigators.

IV.A.2 Assistance with searches and evidence obtained by public investigating authorities during an investigation

When investigating authorities execute a search warrant to obtain evidence, they will often rely on IP owners to assist in evaluating this evidence. In some instances, IP owners will be provided access to the seized evidence after-the-fact, and they can help investigating authorities correctly identify the infringing item, distinguish between types of infringing items, and even better understand better the evidence that they have seized. Some IP owners have created a product verification procedure and even checklists that make it easier for investigating authorities to make these distinctions.

In cases involving the search of physical spaces, such as warehouses or offices, investigating authorities may seek permission from judicial authorities for IP owners to accompany investigating authorities during the execution of the search warrant for the same purposes – namely to help investigating authorities better identify and understand the evidence. IP owners can participate in the execution of the search warrant when investigating authorities can ensure the safety of the IP owner. Where public investigating authorities cannot ensure IP owners' safety during the execution of a search warrant, they may still ask IP owners to be 'standing by' until the searched location can be secured. Once it is, IP owners can safely enter the searched location and assist the investigating authorities.

This approach has an additional benefit for investigating authorities – it may make it easier for them to limit the volume of their seizure. For example, a search of a warehouse in a counterfeit goods case may yield counterfeit goods, non-counterfeit infringing goods, and non-infringing

goods. Without the expertise of an IP owner at the scene of the search, investigating authorities may be inclined to seize everything until they can properly distinguish between the various types of seized goods. This can create a storage problem, as the goods seized can number in the hundreds of thousands. Having IP owners present at the scene of the search enables investigating authorities to take advantage of the IP owners' expertise in distinguishing between these types of goods, thereby allowing investigating authorities to seize only those goods that truly violate the criminal counterfeiting laws.

IV.A.3 Chain of custody documentation

Once investigating authorities begin their criminal investigation, they often seek to replicate what the IP owner discovered when it put together its criminal referral. For example, when an IP owner makes a test purchase or download, investigating authorities may endeavour to make the same test purchases or downloads and use such evidence in their case – including at trial – rather than use the evidence that the IP owner itself has gathered.

However, investigating authorities may instead choose to rely on some of the test purchases or downloads made by IP owners to build their case. Investigating authorities may even rely on the IP owners' test purchases or downloads at trial. In such cases, investigating authorities may ask IP owners to provide documentation establishing the chain of custody for the test purchase or download. Establishing this chain of custody is helpful for investigating authorities because it allows a prosecutor to argue at trial that a judicial authority can place greater weight on such evidence and rely on it. In this sense, documenting chain of custody to support a trial in a public criminal IP case is no different than when an IP owner presents such documentation at trial in a civil or private criminal IP case – *i.e.*, to show that the evidence obtained during a test purchase or download is reliable.

To document chain of custody for in-person test purchases in physical markets, it is helpful for the IP owner to take photographs of:

(1) the infringing product being offered for sale;

(2) the location and the seller of the infringing product being offered for sale;

(3) the infringing product upon purchase;

(4) if it is in packaging, the product upon opening the packaging, to show that it is the same as the products offered for sale; and

(5) the secure evidence location where it is stored.

If possible, the IP owner can make a video of the same chain of custody process. The name of the IP owner's investigator making the purchase, the date of the purchase and storage of the infringing product, and the location of the infringing product since its purchase can all be documented. If, at some later time, other IP owner investigators handle the infringing product, then the names of these investigators, the dates when they accessed the infringing product, and any other locations where the infringing product may have been stored can all be documented as well. In this way, the chain of custody documentation can establish that the IP owner knew at all times who was in contact with the evidence, when the contact occurred, and where the evidence was stored.

To document the chain of custody for test purchases made online, IP owners can take many of the same steps previously identified in discussing the gathering of evidence for a criminal referral for online test purchases (see 0 0above). Specifically, IP owners can take screen shots of the infringing product being offered online, as well as screenshots of the final sale. IP owners can use video software to document the online sale as well. Once the product is received by courier delivery or through the post, then the same chain of custody documentation steps outlined above for purchasing a physical product can be taken.

To document the chain of custody for test downloads or streams, the chain of custody documentation will include some of the same information previously discussed that IP owners can gather during a test download (see II.B and 0 above). For example, the IP owner can take screen shots to document the offer of an infringing download or stream and the completion of the transaction – as well as every step in between. IP owners may also use specialised software to make a video recording every step the IP owner took online when making the test purchase or download. The IP owner can also document on which server the test download is stored and log every time the file is accessed.

IV.B Guidelines specific to copyright cases

Copyright owners can play a multi-faceted role during a criminal investigation. For instance, because most countries do not offer registration of copyrights, copyright owners will have to provide witness statements and other evidence establishing the validity of the copyrights alleged to have been infringed. As already noted, some copyright owners rely on registrations made in countries that do offer the option of registering a copyright to support any witness statements concerning copyright validity.

During a criminal copyright investigation, investigating authorities may also ask copyright owners to evaluate infringing copies of copyrighted works to verify that they are, in fact, copies of the copyrighted works in question. This request could occur in the context of test purchases or downloads made by the copyright owners, or it could also occur after investigating authorities have made their own test purchases or downloads. For example, in a music piracy investigation, investigating authorities may ask copyright owners to confirm that an infringing copy of an album is, in fact, a copy of the copyrighted work that the infringing copy purports to be. Copyright owners could themselves listen to the album to make this comparison, or they can use software to accomplish the same task. In the same vein, investigating authorities investigating a movie piracy case may ask copyright owners to view the infringing copies of the movies to verify that they are, in fact, copies of the copyrighted work in question.

Investigating authorities may also ask copyright owners to assist in establishing an infringer's knowledge during the investigation. Most countries have some form of notice-and-stay-down (*e.g.*, the EU Copyright Directive) or notice-and-take-down procedures (*e.g.*, the U.S. Digital Millennium Copyright Act) the copyright owners may use to notify infringers that they are distributing infringing copies or streaming infringing performances online. In some instances, copyright owners refrain from using these notice procedures when they know they will be referring the case to investigating authorities. In these situations, investigating authorities may ask the copyright owner to implement one of these notice procedures before investigating

authorities make a test download or stream to help establish the infringer's knowledge that what they are doing is illegal.

In addition, investigating authorities may ask for witness statements related to the retail value of a copyright work at the time of the offence. These statements may specify the retail value at a particular point in time for the online market where the criminal copyright case is being investigated.

IV.C Guidelines specific to trade mark cases

During a criminal trade mark counterfeiting investigation, investigating authorities may ask trade mark owners to provide statements related to the validity of the trade mark, beyond the certified copy of the trade mark registration that is likely to have been provided already as part of the criminal referral. Such statements could include when the trade mark owner used the trade mark on the same class of goods on which the defendant has used the counterfeit mark. The statement may also include both personal knowledge and descriptions of other evidence such as catalogues or other advertisements showing the offer of goods bearing the registered trade mark at the time of the offence.

The witness statements can also include information about the goods themselves that establishes when a good bearing the registered trade mark is not authentic – something that can be helpful after a test purchase or in the execution of a search warrant. For example, a brand owner that manufactures purses bearing a registered trade mark may only use gold zippers on the authentic purses that it makes. If the defendant uses silver zippers on the purses bearing the counterfeit mark, then the trade mark owner's statement could specify that this is one easy way (of, perhaps, many) for investigating authorities (and judicial authorities) to quickly establish that the goods at issue are not authentic.

Investigating authorities could also ask brand owners to provide witness statements related to the labels and documentation that accompany authentic goods bearing the trade mark owner's registered trade mark. Such statements could include what documents or labels typically accompany authentic goods bearing the registered trade mark – another way in which investigating authorities could quickly determine whether a good is authentic. These statements could also help investigating authorities independently identify a counterfeit label.

IV.D Guidelines specific to trade secret cases

Investigating authorities may ask trade secret owners during a criminal trade secret investigation to provide additional information establishing that the misappropriated property at issue qualifies as a trade secret. Often, such additional information relates to the purpose or role of the trade secret in the business and can be easily provided through in-house expert guidance to investigating authorities. For example, an in-house expert with the trade secret owner could explain why a soft drink formula or popular food recipe is unique and confirm that

it has not been reverse engineered by competitors. In this way, a trade secret owner can reveal additional facts without revealing the trade secret itself.

Occasionally, investigating authorities may need to learn of the trade secret itself to confirm its trade secret status. In such cases, trade secret owners can enter into a 'protective agreement' with investigating authorities (that could be submitted under seal and enforceable by a judicial authority) to provide added protections limiting which law enforcement officers and prosecutors may have access to the trade secret, restricting how it can be used or discussed, and providing a court-supervised mechanism to resolve any disputes. Such disclosures to investigating authorities do not cause the trade secret to lose its secret status.

During a criminal trade secret investigation, investigating authorities could also ask the trade secret owner to provide more access to employees and to servers or networks – particularly if the trade secret is in digital form. Investigating authorities may ask for logging information – key card logs of those who have entered a secured space or logs offer those who have accessed a secured server housing a digital trade secret. Investigating authorities may also ask for additional information to understand the value of the trade secret.

Finally, investigating authorities may ask for further information regarding the measures that the trade secret owner took to protect the trade secret – whether they be physical, electronic, or company policies and practices. Examples of such protection measures are set forth in II.D.

V Role of IP owner during the court proceedings

V.A Generally applicable guidelines

IP owners continue to play a role in an IP crime case after the commencement of court proceedings. Such proceedings may commence when someone is arrested on IP crime charges or when the government obtains an indictment charging a defendant with an IP crime. The role of the IP owner can become particularly important during evidentiary hearings, trial, and sentencing hearings when IP owners testify as witnesses. IP owner testimony can be broad in scope – touching on almost every element of the IP crime at issue.

V.A.1 Testimony of valid IP, infringement (e.g. digital content, counterfeit goods), and value

For example, IP owners typically must testify regarding the validity of the particular IP at issue – be it a copyright, trade mark, or trade secret. Prosecutors may also ask the IP owner to provide fact or expert testimony explaining why the infringing items in the case are not authentic. This testimony could cover differences in quality, the packaging used, and other differences that would make it clear to a judicial authority that the infringing item is not authentic.

In addition, IP owners could be asked to testify about test purchases or downloads made by their investigators. This testimony could include an explanation of how the IP owner targeted the defendant for investigation, as well as what steps the IP owner took to make test purchases, authenticate the photographs or screenshots that the IP owner took or made, and authenticate the infringing items purchased or downloaded by the IP owner. The IP owner may also be asked about the chain of custody to assess the reliability of the test purchase or download.

Some IP owners find it useful to use the same employee or investigator to testify in a particular country or region to minimise the likelihood of inconsistent testimony. Some IP owners may even use the same person to testify in cases throughout the world. Sometimes IP owners will use the same outside expert to testify about how infringing items are identified.

IP owners may also testify about the harm caused by the IP crime involved. Sometimes that testimony can centre on the value of the IP that has been infringed. At other times, it can focus on the damage caused to an IP owner's business model, reputation, or even the business's very viability.

V.A.2 Claim for damages

Most IP owners are given the opportunity – at trial, at a sentencing hearing, or both – to make a claim for damages or restitution for the pecuniary harm caused by the IP crime. IP owners may even be permitted to make the same statutory damages claim that they could make in an analogous civil IP case. IP owner claims for damages are typically assessed under the civil standard of proof (rather than the higher criminal standard of proof) when they are made after a defendant has been convicted of an IP crime.

IP owners who wish to make claims for damages can consider gathering the same information that they would for a civil IP case. They can also consider hiring an outside attorney to represent them in court proceedings to present this evidence and even call witnesses, where permitted, to authenticate and present the relevant and necessary evidence for a damages claim.

V.B Guidelines specific to copyright cases

During court proceedings in a criminal copyright case, copyright owners can expect to be called upon to testify about the validity of the copyrights alleged to have been infringed. Copyright owners may provide testimony explaining why the content they created or owned constitutes original expression fixed in a tangible medium. As already noted, some copyright owners rely on registrations made in countries that do offer the option of registering a copyright to support any witness statements made to show copyright validity, and copyright owners can testify to these registrations as well.

Copyright owners may also offer testimony explaining how they determined that the items seized, downloaded, or streamed in the case are infringing copies of the copyrighted works. This testimony could relate to test purchases or downloads by the copyright owners themselves or by investigating authorities. For example, in a music piracy case, copyright owners could testify that they listened to, or used software to analyse, a downloaded album to confirm that it is an infringing copy of the authentic copyrighted work that the infringing copy purports to be. Similarly, prosecutors may ask copyright owners to view the movies at issue in a movie piracy case to verify that they are, in fact, infringing copies of the copyrighted work.

Copyright owner testimony could also include an explanation of how they gathered attribution and identification evidence establishing that the infringing item came from the infringer – such as the authentication of screenshots and evidence tracking IP addresses during a test download or stream.

At trial, prosecutors may ask copyright owners to provide testimony that could help establish the defendant's knowledge of the copyright crime. This testimony could include an explanation of the various forms of notice a copyright owner may have previously provided to the defendant of copyright infringement – such as a cease-and-desist letter, a takedown or stay-down notice, or a prior civil complaint filed against the defendant. The testimony may also include what responses were received from the defendant, if any, as well as any testimony about whether the defendant's conduct changed post-notice.

In addition, prosecutors may ask copyright owners for testimony related to the retail value of a copyrighted work at the time of the offence. This testimony may include the specific retail value of the copyrighted work at a particular point in time on the online market where the criminal copyright case is being investigated.

V.C Guidelines specific to trade mark cases

Once court proceedings have commenced, trade mark owners may have to play a multi-faceted role. They are often presented as witnesses to introduce certified copies of the registered trade marks relevant to the criminal trade mark counterfeiting case. Prosecutors may also ask trade mark owners to testify about whether the registered trade mark was in use at the time of the counterfeiting crime and on the same class of goods on which the defendant used the counterfeit mark. Trade mark owners may also authenticate catalogues, annual

reports, or other documents introduced into evidence to supplement personal knowledge establishing when the registered mark was in use.

Prosecutors may ask trade mark owners to offer testimony explaining why the goods trafficked by the defendant are not authentic. This testimony may focus on the differences in quality, price, style, colour, or other aspects that show that the defendant's goods are not authentic. This testimony can also include an explanation of the differences in the labels or packaging intended to accompany the goods.

For certain types of goods, such as counterfeit pharmaceuticals or perfume, trade mark owners may offer testimony of lab testing showing that the defendants trafficked in drugs or perfumes that are not authentic. For example, a scientist employed by the trade mark owner may testify to mass spectroscopy or thin layer chromatography demonstrating that the defendant's goods contain ingredients not found in the authentic drugs or perfumes.

At trial, prosecutors may ask trade mark owners to provide testimony that could help establish the defendant's knowledge of the trade mark counterfeiting crime. This testimony could include a description and authentication of cease-and-desist letters or takedown notices that the trade mark owner sent to the defendant. The testimony may even include a prior civil complaint filed against the defendant. It is not uncommon for trade mark owners to testify to the notices that they received from customs authorities after they seized a defendant's goods because they were alleged to have borne counterfeit marks. This testimony may also include what responses were received from the defendant, if any, as well as any testimony about whether the defendant's conduct changed post-notice.

In addition, and especially during a sentencing hearing, prosecutors may ask trade mark owners for testimony related to the retail value of the goods bearing the registered trade marks at the time of the offense. This testimony may include the specific retail value of the goods bearing the registered trade mark when the counterfeit trade mark crime occurred.

V.D Guidelines specific to trade secret cases

During criminal court proceedings, prosecutors may ask trade secret owners to offer testimony establishing that the misappropriated property at issue qualifies as a trade secret. Often, such testimony is provided by an expert in-house to the trade secret owner in a way that describes what the trade secret's function is and why it is valuable to the owner. This approach avoids the risk of revealing the trade secret itself. For example, the trade secret owner's in-house software programmers could explain why their algorithm for high-frequency stock trading the fastest known algorithm on the market is - without disclosing the algorithm itself. They could explain why having the fastest algorithm allows them to make trades at advantageous prices before competitors can.

After an indictment, trade secret owners may be required to disclose the trade secret to defendants' counsel to allow defendants to make a fair challenge to the property's putative trade secret status at trial. In such cases, trade secret owners (and prosecutors) can ask the judicial authorities to issue a protective order prior to disclosure. Such a protective order could

place limits on what information is disclosed, to whom, and how and where it can be reviewed. Specifically, such a protective order could include the following:

- Identifying what information, the trade secret owner deems to be trade secret information, even if the defendant intends to dispute this assessment
- Restricting access only to certain of the defendants' counsel or counsel's staff
- Restricting access to certain locations, such as the prosecutor's office, law enforcement offices, or even the trade secret owner's office
- Providing a procedure for handling the information, such as limiting the review to paper form or to a computer or device not connected to the internet
- Requiring defendants' counsel and counsel's staff to store copies of putative trade secret materials in locked compartments such as a filing cabinet or on an encrypted password-protected computer
- Requiring that recipients of the putative trade secrets sign certifications that they will comply with the protective order
- Remedies for violations of the protective order

During trial, other protective measures could be added to a protective order. For example, the trade secret owner could ask that certain "code words" be used for certain terms or ideas that, if revealed, would jeopardise the secrecy of the trade secret. If code words or other precautions are insufficient, then the trade secret owner could even ask that the courtroom be sealed, and every participant in the trial be subject to a gag order subject to penalties by a judicial authority. A trade secret owner could also ask the court to seal any exhibits related to the trade secrets and then have them destroyed once all appeals are exhausted.

In addition, prosecutors may ask trade secret owners to testify about the measures that they took to protect the trade secret – be they physical, electronic, or company policies and practices. Examples of such protection measures are set forth in II.D.

VI Factors to consider after the court decision(s)

VI.A Generally applicable guidelines

Access to evidence for subsequent use in civil court cases

Factors to consider after the court decision(s)

Help with storage and destruction

VI.A.1 Access to evidence for subsequent use in civil court cases

Once a case is concluded, courts are often required to forfeit and destroy all the infringing items in the case. In countries where courts are not so required, it is common for the IP owner to demand the destruction of the counterfeit goods at the infringer's expense, as well as the equipment used for its production at the end of the criminal IP case. However, there are instances when IP owners may prefer to preserve access to this evidence.

Most commonly, this occurs when the IP owner is unsuccessful in obtaining restitution or other civil damages within the criminal proceedings and wishes to pursue its own, additional, civil IP case. In such circumstances, preserving access to evidence used in a criminal IP case can be vital for the IP owner's prospects in a civil case.

To ensure access to such evidence, IP owners often retain outside counsel to file a request to preserve the evidence with the judicial authority overseeing the criminal IP case for use in a future civil IP case. Before submitting such a request, IP owners can consider the storage costs for such infringing items, which can be quite high in large-scale cases and are likely be paid by the IP owner after the court decision.

An IP owner's request to preserve access to evidence may include a request to suspend any destruction order until the conclusion of the civil IP case. If the IP owner only needs a sample of the evidence, then IP owners can include this point in their request. As discussed more fully below, IP owners may wish to consider requesting only samples of the infringing items to save on storage and destruction costs.

VI.A.2 Help with storage and destruction

Although the issue of storage and destruction must be decided following a court decision in a criminal IP case, it starts after the first seizure in a case. Some seizures have included more than 20 tons of counterfeit goods. Requirements and practices related to the storage and destruction of infringing goods vary widely from country to country.

A few countries will not conduct a seizure unless and until the IP owner provides assurances that it is able to pay for storage costs during the criminal investigation and court proceedings as well as destruction costs after the court decision. When considering a criminal referral in such countries, IP owners can determine whether they are willing to pay these costs prior to making the referral. If they are so willing, then they can ask the appropriate authorities to preserve the evidence.

In most countries, however, the government pays for the costs of storage and destruction of infringing items involved in a criminal IP case until its conclusion. Some government authorities, particularly customs authorities, have strict timelines for how long they will store infringing items before they order their destruction. Storage costs can be very high in large-scale IP cases, and the government does not want to pay for storage for longer than it has to. For this reason, some investigators and prosecutors may ask IP owners to assist in identifying the proper samples necessary for the criminal case, so that the government can destroy the bulk of the infringing items.

As discussed above, IP owners may consider presenting their own request to customs or other authorities to preserve the evidence for use in a subsequent civil IP case. In so doing, an IP owner may be asked to pay for the storage and destruction costs, and the IP owner will typically be considered the custodian of the evidence at that point. Again, sampling is one way IP owners can minimise storage costs for such evidence during a subsequent civil IP case. In many countries, if the IP owner has a representative number of samples and documents through photographs and witness testimony what the total number of infringing items was, then the IP owner will not have to present all the infringing items in a subsequent civil IP case.

In general, IP owners who decide to pay for storage costs may also consider the quality of the storage facilities. For example, some infringing items may need to be kept within a certain temperature range, so a storage facility with temperature controls may be needed. Storage facilities can also be targeted by IP criminals seeking to steal the infringing items and then traffic in them. Thus, IP owners may consider how secure a storage facility is before selecting one.

Regarding the destruction of infringing items, IP owners can consider the environmental impact of such destruction. Some countries may have laws or regulations that require IP owners to destroy infringing items using certain environmentally friendly methods. Newer methods for destruction are being developed, and IP owners can consider referring to, and keeping up to date with, the latest methods for the ‘clean’ destruction of infringing items.

VII Perspectives

The guide has laid out a series of general guidelines for criminal referrals in IP cases building on experiences from IP owners from numerous sectors and geographical areas. However, the guidelines are merely suggestions, and seldom are two cases the same and there is no such thing as a perfect case.

As reflected in the interviews with IP owners and their representatives, the **following good practices have been identified:**

1. **Facilitate good preparation of criminal referrals.** Establish trustworthy brand protection procedures within the company, such as regular market monitoring to collect data, information intelligence, and evidence.

2. **Make a comprehensive package of information, evidence, and legal background.** Law enforcement and prosecutors handling IP crime cases are not always experienced in the field, and it can be an advantage to make sure that the terminology and legal framework is explained thoroughly.

3. **Cooperation between IP owners through trade associations and law enforcement authorities or other stakeholders.** Advantages include the opportunity to combine different trade association members' infringements, have various monitoring efforts, and building national and international networks which may help in more efficient detection of IP infringement.

4. **Establish a good relationship with law enforcement, whether informal or formal**. IP owners should always be readily available so officers can obtain the necessary information quickly.

In addition, IP owners and their representatives identified the following obstacles to effective enforcement:

1. **Law enforcement and prosecutors do not always recognise the importance of IP crime.** There are many reasons why this may happen. Deterring IP crime may not be a priority in every jurisdiction. And even where it is a priority, some jurisdictions do not have the resources to devote to more than just a few IP cases a year. Jurisdictions where the penalties for IP crimes are low also makes it harder for investigative authorities in such jurisdictions to prioritise IP crime cases.

2. **While large companies can easily afford to finance market monitoring, private investigators, lawyers or storage of infringing goods, SMEs lack the resources.** SMEs are often targets of IP crime and the negative effects can be very serious as their business can easily collapse after only a few targeted infringement cases.

3. **In many jurisdictions, the thresholds for starting a criminal case are high.** Even if some cases are potentially significant, it can sometimes be difficult to provide necessary documentation from the beginning.

4. **Jurisdictional issues can be hard to overcome when crimes are committed across borders.** It is increasingly common that IP criminals apply complicated cross border offline and online infrastructures, supply chains, and money transfers.

5. **Too low a level of international collaboration between authorities, both within countries, across the EU and outside Europe.** While international cooperation has improved over recent years, stronger international cooperation would be highly beneficial.

Annex

Annex 1 – Frequently asked questions (FAQ)

Answers to 8 questions frequently raised concerning IP crime cases and the role of the IP owner are given below.

1. Is IP infringement always a criminal offence?

Whether a particular infringement of an IP constitutes a crime and satisfies the requirements for investigation and subsequent prosecution always depends on national legislation. In most countries, criminal penalties can be imposed on those who commit wilful trade mark counterfeiting and copyright piracy on a commercial scale, but many countries are also imposing criminal penalties on other types of IP infringement. For this reason, IP owners, private as well as public investigators, and prosecutors should be aware of national differences in the variety of IP crimes that may be investigated and prosecuted and how these differ depending on the country.

2. How does an IP owner determine whether a particular infringement of an IP warrants a criminal referral?

When deciding whether to make a criminal referral, IP owners may consider several factors – especially those that investigating authorities prioritise in deciding whether to accept a criminal referral for investigation. IP crimes with the highest impact on the IP owner and the public often warrant a criminal referral because they are most likely to be a high priority for investigating authorities. For example, IP crimes implicating public health and safety typically warrant a criminal referral. An organised crime group being responsible for the particular IP crime is another factor that weighs heavily in favour of making a criminal referral. Sometimes, the IP owner will also choose to make a criminal referral if the means necessary to investigate the IP crime is only available to a public investigating authority.

3. Where does an IP owner report a suspected IP crime?

In most cases, countries use their own national authorities to investigate and prosecute IP crimes, generally through the police and the public prosecution service. These national authorities usually have specific mechanisms in place for reporting and investigating IP crimes within their jurisdiction. Reporting IP crimes to the relevant national authorities is the main step in initiating the legal process and enforcement actions. Once a national authority accepts a criminal referral for investigation, the case will usually involve the public investigating authority choosing an investigation strategy, conducting a preliminary investigation, executing a search or multiple searches on an ‘action day’, finalising the investigation, followed by an indictment and the court proceeding itself.

4. What information can an IP owner gather as part of its private preliminary investigation for possible inclusion in a criminal referral?

Although a private preliminary investigation conducted by an IP owner is not a substitute for a formal criminal investigation, the IP owner can use a private preliminary investigation to gather important information. During this private preliminary investigation by the IP owner, several broad categories of information could be gathered, such as an analysis of the infringing item(s) obtained through a test purchase, financial information related to the purchase, and identifying information attributing the IP crime to a particular group or individual. Information can be gathered by IP owners through various methods and from various sources. This can be achieved through multiple strategies, such as observing or monitoring suspected illegal activity, and conducting a lawful online investigation into suspected IP criminals to obtain open-source intelligence (OSINT) and social media intelligence (SOCMINT). IP owners sometimes retain professional investigation services and specialised lawyers or firms to assist in gathering this information.

5. What information can an IP owner include in a criminal referral?

The initial referral package should contain sufficient detail to identify the IP owner and other victims of the crime, explain what crimes are involved, where and when the crimes occurred, who (if known) committed the crimes, why the IP owner chose to refer this particular case, and why investigating authorities should accept the referral for investigation. Although it is not usually necessary to include every conceivable detail, IP owners often offer to provide more complete details to investigating authorities at their request. In cases where the investigating authority is not familiar with IP crime, the criminal referral can contain an explanation of IP related issues, including an explanation of how the national IP laws may apply to the IP crime in the criminal referral.

6. How does an IP owner's behaviour change after making a criminal referral?

How an IP owner's behaviour may change after making a criminal referral may depend on the targets of the IP investigation. An IP owner may not wish to send a cease-and-desist letter or a takedown notice after deciding to make a criminal referral – although the IP owner might otherwise do so in the normal course of confronting infringers – because the IP owner may not want to 'tip-off' the targets that they are under investigation. Similarly, investigating authorities may advise IP owners that they are considering a criminal investigation and may ask the referring IP owner not to take any action that may alert the targets that they are under scrutiny. On the other hand, the targets of the IP investigation may very well be the subject of a criminal referral precisely because the targets have already received dozens of cease-and-desist letters or takedown notices and have chosen to ignore them. In this situation, an IP owner's behaviour may remain unchanged.

7. What is the role of an IP owner during the criminal investigation and the court proceedings?

Once the criminal investigation has begun, it is unlikely that the IP owner's role will end. When investigating authorities conduct searches to obtain evidence, they will often rely on IP owners to assist in evaluating this evidence. In some instances, IP owners will be given access to the seized evidence after the fact, and they can help investigating authorities correctly identify the infringing items, distinguish between types of infringing items, and gain a better understanding of the evidence that they have seized. If the IP owner has conducted a test purchase, investigating authorities may ask IP owners to provide documentation establishing the chain of custody for the test purchase or download. IP owners can also continue to play a role in an IP crime case after the commencement of court proceedings. The role of the IP owner can become particularly important during evidentiary hearings, trials, and sentencing hearings when IP owners testify as witnesses. IP owner testimony can be broad in scope – touching on almost every element of the IP crime at issue.

8. Can an IP owner claim damages during a criminal proceeding?

In many cases, the IP owner can make a claim for civil damages (often called 'restitution') as part of the criminal proceeding – usually during or after the sentencing phase. Many jurisdictions even authorise IP owners to bring a civil proceeding for damages in parallel to the criminal proceeding. More often, jurisdictions authorise IP owners to bring a civil proceeding for damages against an IP criminal after the criminal prosecution has ended. In anticipation of this type of civil proceeding, it is important for an IP owner to ensure that any evidence used in the criminal proceedings that the owner may need for a subsequent civil claim for damages is preserved. Typically, either the public prosecutor or the IP owner will file a formal motion or request asking the judicial authority overseeing the criminal proceeding to preserve any evidence needed for a later civil proceeding for damages.

Annex 2 – Criminal referral checklist

Criminal Copyright and Trade mark Infringement

1. *Victim's contact information*

Consider providing the names, titles and contact information of all people with knowledge of information that could be helpful to law enforcement.

- → Name
- → Address
- → Nature of business
- → Primary address
- → Work phone
- → Mobile phone
- → E-mail
- → Fax

2. *Intellectual property description*

- → Describe the copyrighted material (e.g., title of copyrighted work), including whether infringement of the work poses a particular harm to the copyright owner (e.g., pre-release piracy), and why the material includes original expression fixed in a tangible medium.
- → Describe the trade mark or service mark (e.g., the logo, design, or word mark), including whether counterfeiting the trade mark could cause a significant public harm (e.g., threats to public health and safety).
- → Is the mark registered with a national IP Office or the EUIPO?
  Yes ☐ No ☐
- → If yes, please provide the following:
  - Offices where the trade mark is registered
  - Registration number
  - Registration date
  - Registered goods and services, incl. class of goods and services
  - Dates when the trade mark owner used the trade mark on the class of goods or services in the registration.

→ Do you have a certified copy of the certificate of the trade mark registration(s)?
Yes ☐ No ☐

→ What is the approximate retail value of the infringed work, authentic good, or authentic service?

→ Has the work or mark been the subject of a previous civil or criminal enforcement action? If so, please provide a general description as well as the country, case name, case number, and the name of the court.

3. *Suspected intellectual property crime description*

→ Describe how the infringement or counterfeiting was discovered.

→ Describe how the IP owner knows that the infringing items are not authentic.

→ Do you have any examination reports of the infringing downloads or streams obtained during a test download or stream, or examination reports of counterfeit goods obtained during a test purchase?
Yes ☐ No ☐

If yes, please provide those reports to law enforcement. If possible, please also provide a screenshot, video, photograph, or sample of the goods.

→ Describe the type of copyright infringement (e.g., reproduction, distribution, or public performance (such as streaming)).

→ Describe the type of trade mark counterfeiting (e.g., manufacture, reproduction, import, export, or distribution).

→ Describe the scope of the infringing or counterfeiting operation, including the following information:
- Estimated quantity of illegal distribution:
- Estimated value of illegal distribution:
- Estimated time period of illegal distribution:
- Is the illegal distribution national or international? Which states/provinces and/or countries?
- Identify where the infringement or counterfeiting occurred and describe the location.

→ Do you have any examination reports of counterfeit labels or packaging?
Yes ☐ No ☐

If yes, please provide those reports to law enforcement. If possible, please also provide a photograph or sample of the counterfeit labels or packaging.

→ Have you received any customer complaints about the infringing items or counterfeit goods distributed by the possible suspect(s)?
Yes ☐ No ☐

If yes, please provide copies of those complaints to law enforcement as well as a description of how the IP owner received the complaint (e.g., directly from the customer) or observed the complaint (e.g., on the website of the possible suspect).

→ Do you have any reports or documents (e.g., receipts or invoices) related to the tracking of payments during a test purchase?
Yes ☐ No ☐

If yes, please provide those reports or documents to law enforcement.

→ Do you have any evidence of other crimes (e.g., money laundering, computer hacking, or fraud) that the suspects committed along with the alleged IP crimes?
Yes ☐ No ☐

If yes, please provide any documents or other evidence about these other crimes.

4. *Origin and entry*

→ Identify the country of origin of the infringing item.
→ Identify the date, location, and mode of the item's entry into the country.
→ Identify the names of shippers and provide any other applicable shipping or customs information.

5. *Possible suspects*

→ Identify the name(s) or location(s) of all possible suspects, including the following information:

- Name
- Phone number
- E-mail address
- Physical address
- IP address
- Current employer, if known
- Reason for suspicion
- Businesses or entities related to the suspect
- Websites related to the suspect
- Any other identifiers

6. *Role of the internet*

→ If the distribution of copyright infringing or counterfeit trade mark goods involves the Internet, identify the following:

- Elements related to the Internet (e.g., websites, FTP, mail, or chat rooms)
- Relevant Internet address, including any affiliate websites (e.g., domain names, URLs, IP addresses, e-mail addresses)
- Login or password for website
- Operators of website, if known:

→ Location of the servers and website host

→ Country where the domain name is registered

- Has the IP owner sent a cease-and-desist notice to the website?

Yes ☐ No ☐

If yes, please provide the following:

→ Date of notice:

→ Do you have a copy of the notice? Yes ☐ No ☐

- If you have conducted an internal investigation into the copyright infringement or trade mark counterfeiting activities, please describe any evidence acquired and submit, if possible, any investigative reports.

7. Civil enforcement proceedings

→ Have you ever received counterfeit goods from the target listed above?

Yes ☐ No ☐

If yes, did you notify the target that the goods received were counterfeit?

→ Has a civil enforcement action been filed against the suspects identified above?

Yes ☐ No ☐

If yes, identify the following:

- Name and location of court and case number
- Date of filing
- Names of attorneys
- Status of case

If no, please state whether a civil action is contemplated, what type and when.

→ Have you contacted any other government agencies in any country about this incident?

If yes, identify the agency contacted.

→ Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

Trade Secret Offences

1. *Victim's contact information*

Consider providing the names, titles and contact information of all people with knowledge of information that could be helpful to law enforcement.

- → Name
- → Address
- → Nature of business
- → Primary address
- → Work phone
- → Mobile phone
- → E-mail
- → Fax

2. *Description of the trade secret*

- → Generally describe (without disclosing) the trade secret (e.g., source code, formula, technology, process, or device), and explain how that information differs from that disclosed within any issued patents and/or published patent applications.
- → Provide an estimated value of the trade secret using one or more of the methods described in the table below.

Method	Estimated value
Cost to develop the trade secret	
Acquisition cost (include date/ source of acquisition)	
Fair market value if sold / licensed	

3. *Measures taken to protect the physical trade secret location*

→ Describe the company's general security practices concerning entry to and movement within its premises, such as fencing the perimeter of the premises, visitor control systems, or the use of alarms, or self-locking doors or security personnel.

→ Describe any security measures the company has employed to prevent unauthorised viewing of or access to the trade secret, such as requiring a security escort for visitors, video surveillance, locked storage facilities, or 'Authorized Personnel Only' signs at access points.

→ Describe any protocol the company employs to keep track of employees accessing trade secret material, such as sign in/out procedures for access to and return of trade secret materials.

→ Are employees required to wear identification badges?
Yes ☐ No ☐

→ Does the company have a written security policy?
Yes ☐ No ☐

If yes, please provide the following information:

- Does the security policy address in any way protocols on handling confidential or proprietary information?
  Yes ☐ No ☐
- How are employees advised of the security policy?
- Are employees required to sign a written acknowledgement of the security policy?
  Yes ☐ No ☐
- Was access to the trade secret limited to a "need to know" basis?
  Yes ☐ No ☐

If yes, describe how 'need to know' was maintained in any ways not identified elsewhere (e.g., closed meetings, splitting tasks between employees and/or vendors to restrict knowledge).

4. *Confidentiality and non-disclosure agreements*

→ Does the company enter into confidentiality and non-disclosure agreements with employees, business partners and third parties concerning the trade secret?
Yes ☐ No ☐

→ Has the company established and distributed written confidentiality policies to all employees?
Yes ☐ No ☐

→ Does the company have a policy for advising company employees regarding the company's trade secrets?
Yes ☐ No ☐

→ Does the company have a policy for advising company employees on how to handle the company's trade secrets?
Yes ☐ No ☐

→ Does the company have a policy to train employees on how to handle the company's trade secrets?
Yes ☐ No ☐

→ Does the company have an exit interview policy?
Yes ☐ No ☐

If yes, describe what the exit interview includes as it relates to trade secrets (e.g., emphasis on and reminder of the trade secret owner's confidentiality policy, obtaining all company storage devices, confirming the return of all proprietary or confidential information, and reminders of non-disclosure agreements, training and policies related to trade secrets).

5. *Electronically stored trade secrets*

→ If the trade secret is computer source code or other electronically stored information, how is access regulated (e.g., are employees given unique user names, passwords, and electronic storage space, and was the information encrypted)?

→ If the company stores the trade secret on a computer network, is the network protected by a firewall?
Yes ☐ No ☐

→ Is access to the electronically-stored information logged?
Yes ☐ No ☐

→ Is remote access permitted into the computer network?
Yes ☐ No ☐

→ If yes, is a virtual private network utilised?
Yes ☐ No ☐

→ Is the trade secret maintained on a separate computer server?
Yes ☐ No ☐

→ Does the company prohibit employees from using unauthorised computer programs or unapproved peripherals, such as high-capacity portable storage devices?
Yes ☐ No ☐

→ Does the company maintain electronic access records, such as computer logs?
Yes ☐ No ☐

6. Document controls

→ If the trade secret consists of documents, were they clearly marked 'CONFIDENTIAL' or 'PROPRIETARY'?
Yes ☐ No ☐

→ Describe the document control procedures employed by the company, such as limiting access and sign in/out policies.

→ Was there a written policy concerning document control procedures?
Yes ☐ No ☐

If yes, how were employees advised of it?

7. Employee controls

→ Are new employees subject to a background investigation?
Yes ☐ No ☐

→ Does the company conduct regular training for employees concerning steps to safeguard trade secrets?
Yes ☐ No ☐

8. Description of the trade secret's misappropriation

→ Identify the name(s) or location(s) of all possible suspects, including the following information:

- Name
- Phone number
- Email address
- Physical address
- IP address
- Current employer, if known
- Reason for suspicion
- Businesses or entities related to the suspect
- Websites related to the suspect
- Any other identifiers

→ Describe how the misappropriation of the trade secret was discovered.

→ Describe the type(s) of misappropriation (e.g., stealing, copying, drawing, photographing, downloading, uploading, altering, destroying, transmitting, or receiving).

→ If known, was the trade secret stolen to benefit a third party, such as a competitor or another business?
Yes ☐ No ☐

If yes, identify that business and its location.

→ Do you have any information that the trade secret was stolen to benefit a foreign government or instrumentality of a foreign government?
Yes ☐ No ☐

If yes, identify the foreign government or instrumentality and describe that information. If the suspect is a current or former employee, describe all confidentiality and non-disclosure agreements in effect.

9. *Civil enforcement proceedings*

→ Has a civil enforcement action been filed against the suspects identified above?
Yes ☐ No ☐

- If yes, please provide the following information:
- Name of court and case number
- Date of filing
- Names of attorneys
- Status of case

If no, please state whether a civil action is contemplated, what type, and when.

→ Have you contacted any other government agencies about this incident?

If yes, identify the agency contacted.

→ Please provide any information concerning the suspected crime not described above that you believe might assist law enforcement.

EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

Intellectual Property Owner Guide to Criminal Referrals in Intellectual Property Crime Cases