E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/15/8
ORIGINAL: ENGLISH
DATE: AUGUST 3, 2022

Advisory Committee on Enforcement

Fifteenth Session
Geneva, August 31 to September 2, 2022

THE ROLE OF INTERMEDIARIES IN IP ENFORCEMENT

Contributions prepared by the United Kingdom, AIM – the European Brands Association, the International Federation of the Phonographic Industry, DHL Express and Mastercard

1. At the fourteenth session of the ACE, held from September 2 to 4, 2019, the Committee agreed to consider, at its fifteenth session, among other topics, the "exchange of information on national experiences relating to institutional arrangements concerning IP enforcement policies and regimes, including mechanisms to resolve IP disputes in a balanced, holistic and effective manner". Within this framework, this document introduces the contributions of one Member State (the United Kingdom (UK)), two Observers (AIM – the European Brands Association and the International Federation of the Phonographic Industry (IFPI)) and two private entities (DHL Express and Mastercard).

2. The contribution by the UK provides an overview of the Real Deal Campaign for Fake-Free Markets, an industry-funded nationwide initiative to tackle the sale of counterfeit and pirate products, the success of which is rooted in cross-sector partnerships with key private and public organizations concerned with reducing trade in IP-infringing goods.

3. The contributions by AIM and IFPI discuss the vital role played by various types of intermediaries in tackling online piracy and counterfeiting and recommend the adoption of several measures to this end. In particular, the contributions encourage intermediaries to undertake reasonable due diligence in knowing their business customer, to adopt both "notice and stay-down" measures and repeat infringer policies and to proactively collaborate with right holders and enforcement authorities. Concrete examples of actions intermediaries can take, as well as areas where existing actions could be intensified or complemented, are also identified.

4. The contributions by DHL Express and Mastercard enrich this document by providing perspectives of other intermediaries in the fight against IP infringements. Both contributions discuss efforts currently being undertaken by both physical and digital intermediaries to combat IP infringements. These efforts include increasing public awareness on IP infringements, taking proactive action to stop trade in IP-infringing goods and actively collaborating with right holders and public authorities. Both DHL Express and Mastercard have adopted policies and undertaken initiatives to actively combat IP infringements, both on and offline.

5. The contributions are in the following order:

[Contributions follow]

REAL DEAL: A COLLABORATIVE APPROACH TO TACKLING INTELLECTUAL PROPERTY CRIME AT MARKETS IN THE UNITED KINGDOM

Contribution prepared by Ms. Patricia Lennon, Campaign Manager, Real Deal Campaign for Fake-free Markets, National Markets Group for Intellectual Property Protection, London, United Kingdom[*]

ABSTRACT

This document provides a summary of the Real Deal Campaign for Fake-Free Markets, which was established in 2009 as a nationwide initiative to tackle the sale of counterfeit and pirate products at markets in the United Kingdom (UK). Funded by industry, its success is rooted in cross-sector partnership work involving all the key organizations in the UK (in both the public and private sector) that are concerned with reducing the trade in fakes at markets. The heart of the initiative is its voluntary charter, through which market operators make a public commitment to keep their markets fake-free. To date, over 500 markets across the UK have made this commitment. As a result of the Real Deal program's success at physical markets, the core model was replicated in 2018 to tackle the trade in fakes on online and social media selling groups.

I. INTRODUCTION

1. The Real Deal Campaign for Fake-Free Markets[1] is an awareness and education initiative, which was launched in 2009 by the National Markets Group for Intellectual Property Protection (NMG) in the United Kingdom (UK) and which complements the NMG's intelligence-led enforcement work. Together, this combination of targeted enforcement and a preventative program provides a 360-degree strategy for tackling sales of products that infringe intellectual property (IP), including counterfeit goods, pirated goods and goods infringing registered design rights, both at physical UK markets and, more recently, online and through social media selling groups. This presentation will look in detail at the Real Deal program and how it has developed over the past 13 years.

II. A COLLABORATIVE INDUSTRY-FUNDED APPROACH

2. The key to the Real Deal's success is collaborative partnership across a wide range of stakeholders. Firstly, the initiative is only possible because of industry's financial commitment: its total contribution to the project to date is more than GBP 500,000, in addition to funding from the European Union Intellectual Property Office (EUIPO) from 2015 to 2016. The project's current industry sponsors cover a wide spectrum of sectors affected by IP infringement, including: the British Phonographic Industry, Palmer Biggs IP Solicitors, the Premier League, Procter & Gamble, React, Superdry, Surelock, the WRI Group and other brand members of the Anti-Counterfeiting Group. Their financial support has ensured the campaign's longevity and underpins its sustainability for the future.

3. Furthermore, the program is endorsed by all the key stakeholders who have an interest in ensuring fake-free trading, including the Chartered Trading Standards Institute (CTSI), Trading Standards Scotland, the National Trading Standards e-Crime Team (NTSeCT) and the UK Intellectual Property Office. It has been cited as a best practice by UK IP ministers, the EUIPO

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

[1] More information is available at www.realdealmarkets.co.uk.

and organizations representing the interests of owners of IP rights (IPRs), as well as by the National Association of British Market Authorities (NABMA) and the National Market Traders' Federation.

III. HOW DOES THE REAL DEAL WORK?

4. The Real Deal initiative provides UK local authorities with a voluntary, self-regulatory, grassroots approach to tackling the trade in fakes at local markets. The key to its success is its focus on facilitating closer working relationships between individuals or organizations responsible for markets and their local authority trading standards service. Trading standards is the market surveillance authority, and is also responsible for consumer protection and market inspection within the UK. The aim of the initiative is to increase awareness amongst market organizers of their responsibilities to ensure that their markets are fake-free and then to provide them with practical information, resources, guidelines and contacts to help them in this endeavor.

IV. PHYSICAL MARKETS AND CAR BOOT FAIRS

5. The initiative was originally developed in direct response to the growing problem of IP infringement, counterfeiting and piracy at physical markets and car boot fairs. At the heart of the project is the voluntary Real Deal Charter[2], which is signed by both the market operators and their local trading standards service to confirm a joint commitment to working together to ensure fake-free trading. The Charter is underlined by a detailed code of practice which sets out procedures for market operators to implement and abide by in order to display the Real Deal logo.

6. Through the Real Deal, markets are provided with a range of practical resources, including the *How to Stay IP Legal* advice leaflet for market traders, posters, and the Real Deal logo to display. The Real Deal approach and the importance of trademark and copyright protection are also included as one of the key learning modules in the NABMA Diploma in Market Administration. For enforcement officers, there is a separate information resource – *Practical Guide to IP Protection at Markets and Car Boot Fairs* – which is an in-depth compendium of case studies, legal approaches, best practices and template documents.

7. Uptake of the Real Deal Charter has grown year-on-year since it was launched in 2009, and the program is now widely used by local authorities throughout the UK. More than 500 markets have signed up to the Charter, covering thousands of market traders and protecting hundreds of thousands of market shoppers.

V. REAL DEAL ONLINE

8. In 2018, the Real Deal launched a parallel program, the Real Deal Online, which targets digital marketplaces, in particular the growing trade in IP-infringing goods on social media buy–sell groups. The new online initiative, developed by the NMG and the NTSeCT, is a natural extension

[2] More information on the contents of the Real Deal Charter and the Code of Practice is available at http://www.realdealmarkets.co.uk/resources/.

of the Real Deal campaign, given that the model – tried and tested at physical markets – is eminently transferable to the online and social media arena. The focus remains the same:

- make market operators or administrators of social media selling groups aware of their responsibilities and liabilities under IP law;
- facilitate engagement between market operators/selling group administrators and their local trading standards service; and
- encourage market operators/selling group administrators to agree to a code of practice and to display it as a message to buyers, sellers and visitors.

9. The Real Deal Online Code of Practice requires group administrators to accept local trading standards officers as members and to agree to five simple steps:

- prohibit the sale of IP-infringing and other illicit goods[3];
- act on information from IPR owners and their representatives who highlight the sale of illegal goods;
- notify trading standards if group administrators believe that illegal goods are being sold within the group and exclude the sellers of these goods;
- highlight warnings and advice notices posted by trading standards; and
- ensure that all members of the group are aware of its fake-free policy.

10. At the launch of the Real Deal Online program in September 2018, IP Minister Sam Gyimah recognized its value, saying: *"The UK is rich with talented creators and innovators, and we must protect their intellectual property rights both online and offline. Social media can be a force for good, making it easier for users to buy and sell goods. However, with this can come an increase of counterfeit goods and other illegal products. This is why I welcome this initiative that brings together industry, trading standards and local government to help protect legitimate businesses and allow right holders to reap the benefits of their own creations".*

11. A Real Deal Toolkit for enforcement officers has been developed with input from NMG members, the NTSeCT and the CTSI Lead Officers for IP. It contains a ready-made package of guidance and resources to assist local trading standards services in tackling the trade in IP-infringing products on social media groups in their area. A complementary program of training and knowledge-sharing activities for trading standards officers is also being rolled out with support from the National Tasking Group, belonging to National Trading Standards, alongside funding from the Real Deal project's industry partners.

12. Since the toolkit launched, over 100 local trading standards services have requested it and more than 200 individual officers have participated in the training program, demonstrating the thirst for knowledge and practical assistance amongst trading standards officers to tackle this growing problem area.

13. Trading standards services across the country have started implementing the program locally, targeting hundreds of group administrators and reaching hundreds of thousands of users of social media selling groups. As more trading standards services adopt the program, the Real Deal message will spread exponentially, with increasing numbers of buy–sell groups becoming fake-free zones.

[3] This includes illegal grey goods, stolen goods, suspected stolen goods, unsafe goods, tobacco goods (duty unpaid), alcoholic goods (without license), fireworks (sold otherwise than in accordance with code and regulations), offensive weapons and items of a pornographic nature.

VI. POSITIVE OUTCOMES FOR A RANGE OF STAKEHOLDERS

14. In the world of physical and digital marketplaces alike, the Real Deal program delivers benefits to a range of stakeholders:

- It provides **local authorities** with a cost-effective, preventative strategy to recognize and reward market organizers committed to keeping their market sites free of IP-infringing and other illicit products.
- It gives **market operators and selling group administrators** a practical framework and set of procedures to ensure that potential traders in illicit goods cannot gain a foothold.
- It enables **IPR owners and local trading standards services** to focus resources more effectively on markets and selling groups where counterfeiting is problematic.
- It ensures a level playing field for **legitimate traders and local businesses** so that they are not competing against traders in fake goods.
- It offers **consumers** a recognizable symbol for fair trading and fake-free market shopping.

[End of contribution]

THE PERSPECTIVE OF AIM – THE EUROPEAN BRANDS ASSOCIATION – ON THE ROLE OF ONLINE INTERMEDIARIES IN THE FIGHT AGAINST COUNTERFEITING

Contribution prepared by Ms. Marie Pattullo, Senior Manager, Trade Marks and Brand Protection, AIM – the European Brands Association, Brussels, Belgium[*]

ABSTRACT

In order to ensure a clean and fair digital ecosystem for all users, and to protect consumers from being confronted with online offers of counterfeit and other illegal, substandard and non-compliant goods, all supply chain partners – including brand holders and online intermediaries – must play their part. This contribution outlines how online intermediaries can help by exercising appropriate control over those parts of the value chain that are within their purview, through:

- reasonable due diligence to identify their business customers;
- providing, and enforcing, relevant intellectual property (IP) protection provisions in their terms and conditions and effective notice-and-takedown systems;
- employing proactive measures, including technical measures, to prevent offers for illegal goods appearing on their services;
- rapidly (and permanently) removing such offers once identified and prohibiting repeat offenders from accessing their services; and
- providing information about infringements on a proactive basis to law enforcement, including customs and market surveillance, authorities, allowing for effective risk analysis and targeting.

Concrete examples of what intermediaries can do to implement these actions, as well as areas where existing actions could be intensified or complemented, are also identified. Finally, the contribution calls on all actors involved to take action in the fight against counterfeiting.

I. OVERVIEW

1. Given the ever-growing global trade in counterfeits and its effects on everything from consumer and other citizen protections up to national economies, secure employment, the environment and innovative industries, it is often said that what is illegal offline should also be illegal online. AIM, the European Brands Association, believes it is necessary to go one step further: we need to turn that rhetoric into real, practical, effective action.

2. AIM represents over 2,500 branded goods manufacturers, ranging from small and medium-sized enterprises to multinational corporations. None of these companies make, transport, export, import, sell or in any way profit from the trade in counterfeits. While all right holders do what they can to protect their intellectual property (IP), from registration all the way through to litigation, they simply do not have the oversight or control of illicit supply chains that would allow for serious disruption of that trade.

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

3. Hence, all actors involved in the supply chain must play their part in this fight. While this contribution focuses on online partners, we cannot – and must not – forget the role of physical intermediaries, such as shipping and other transport and logistics operators; export, import and freight forwarding agents; customs intermediaries; and postal and courier operators. We are all in this together. Or we should be.

II. THE ONLINE ENVIRONMENT

4. The digital transformation has brought many benefits, but also many risks and challenges, including the exponential growth in online offers of counterfeit and other illegal, substandard and non-compliant goods. Protecting consumers and providing them with trusted, safe and innovative goods is in the DNA of every branded goods manufacturer and should also be embedded in any intermediary and retailer, on- or offline.

5. The pandemic changed behaviour almost overnight, with online interaction and commerce becoming mainstream, and arguably essential, in many regions. Purchasing goods online, whether groceries and other essential products or bored-in-lockdown impulse shopping, became the norm for millions who previously preferred the high street. We also saw huge growth in, and reliance on, business-to-business (B2B) e-commerce since online intermediaries do not only service the business-to-consumer (B2C) market. While legal businesses and public authorities scrambled to balance accessibility with safeguards in e-commerce, and law enforcement battled to keep essential trade flowing, counterfeiters turned their attention to fake personal protective equipment (PPE) and medication, or incorrectly marked their shipping documents and packaging as such, and online offers of counterfeits and frauds using brand names proliferated.

6. Yes, we are all thankful that these online commercial channels exist. Yes, they are likely only to grow. And yes, every brand, every service provider, needs and appreciates relationships with online intermediaries to connect to their business partners and consumers. Which is why we also need to rely on them to play their part in keeping the digital environment safe.

III. WHAT IS NEEDED

7. From the perspective of brand holders, online intermediaries can help to maintain a clean and fair online ecosystem by exercising appropriate control over those parts of the value chain that are within their purview, including:

- reasonable due diligence to identify their business customers (“know your business customer”);
- providing, and enforcing, relevant IP protection provisions in their terms and conditions and effective notice and takedown procedures;
- employing proactive measures, including technical measures, to prevent offers for illegal goods appearing on their services;
- rapidly (and permanently) removing such offers once identified and prohibiting repeat offenders from accessing their services; and
- providing information about infringements on a proactive basis to law enforcement, including customs and market surveillance, authorities, allowing for effective risk analysis and targeting.

8. Online intermediaries are not being asked to engage in general monitoring, but, like any business, they should operate with due diligence. Proactive measures to prevent the exploitation of their networks and services by criminals should be integrated into good business practices, and

willing and active cooperation with affected private sector partners, not least right holders, should be the norm. Verification of business customers' identity is an obvious step in a commercial relationship, on- or offline. In a responsible and mature economy, it is surely not contentious that businesses should not be able to operate and have access to modern, necessary infrastructure without accurately identifying themselves.

9. An effective notice-and-action procedure, allowing both users and right holders to flag illegal content (including a trusted flagger mechanism) should feed algorithms leading to automatic or (where needed) human review and appropriate action. Once content is confirmed as illegal, not only must it be taken down expeditiously (the longer it stays online, the longer the right holders and consumers are defrauded), it should never be allowed back up. Please note this is about counterfeit goods, not opinions or other user-generated content that may need to be assessed under freedom of expression standards. No one would expect a counterfeit product to be taken off the supermarket shelf on Tuesday to be back there on Wednesday. Why is this different online?

10. Right holders are often told that they should join intermediaries' brand protection programs. They do, and some of these programs can be effective. However, online partners then ask for even more details about their products and how to authenticate them. Only a right holder can actually authenticate its own brand, and few, if any, will disclose their covert brand protection methods to another commercial player, especially if they are a potential competitor. Right holders are also frequently asked to (repeatedly) provide evidence and translations – even, as is unfortunately all too common, concerning the same repeat infringers.

11. This information exchange street is rather one-way. Right holders are not asking online players to disclose their algorithms, but it would be helpful to have some useable feedback and intelligence. For example, under the European Union's (EU's) *Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet*[4],signatory platforms cite millions of proactive takedowns for each reporting period, which is great – except right holders do not know what they are, why they were taken down (we don't even know how many were for IP infringement) or even which brands and which sellers are implicated. This compromises onward legal action. Surely it would be more effective if all actors were targeting the same rogue traders?

12. Brand holders are also constantly asked for more and more information from law enforcement engaged in IP enforcement, but it is not possible for them to provide information that they do not have. Brand holders do not have visibility over illicit supply and trading channels. While much of that data is owned by, or visible to, transport and other logistics companies, much could also be provided by online intermediaries – especially to customs who could take action against large containerized shipments at the border before they are split into multiple small shipments and pervade the market. Customs should then log and store data regarding all their detentions, including of small consignments. Realistically, customs officers cannot physically control more than one to two per cent of shipments, so solid pre-arrival information and data is essential to allow for effective risk assessment and targeting.

13. Online B2C commerce has, of course, resulted in an explosion of small parcels, but we should not be misled into believing that all counterfeit products arrive that way, so that should not be the only channel customs need to control. Shipping containers can be filled with small items and parcels to be sent once the container arrives in the port, and they often serve to carry stock to feed sellers' fulfilment centres. If customs have pre-arrival data allowing them to target suspect large consignments, this will reduce the burden on their restricted resources while maximising their success rate in targeting illicit shipments. This should also lead to reduced duty and tax avoidance, thus supporting customs' main duties as protectors and collectors of public revenue.

---

[4] https://ec.europa.eu/growth/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en.

14. The proactive sharing of shipping and related customer data with law enforcement agencies (LEAs) should be standard commercial practice. Platforms, social media, online payment providers, messaging services and postal and courier services know – or should know – their business customers. They should know details of repeat offenders and be able to see linked accounts (e.g., those using the same Internet Protocol addresses or banking details). Those that operate proprietary fulfilment centres and distribution networks have multiple commercial datapoints including manifests and picking lists, which should be proactively shared with law enforcement, within relevant legal parameters. These intermediaries are perfectly placed to not only draft appropriate commercial terms and conditions for their paying customers but also to implement them – including, if necessary, contractual provisions or even insurance contracts to cover any delays in delivery or costs, such as for storage and destruction.

15. Players in the Domain Name System (hosting providers, registries, registrars, proxy service providers, resellers etc.) also have their roles to play. Access to and disclosure of accurate and verified WHOIS data is both in the public interest and necessary for compliance with legal obligations. As an unfortunate but direct result of the methods chosen by the Internet Corporation for Assigned Names and Numbers (ICANN) to implement the EU General Data Protection Regulation (GDPR), we are confronted with an almost blanket redaction of domain name registrant data going far beyond that which is necessary. For instance, there is no reason for legal persons' data – to which the GDPR does not apply – not to be collected and disclosed. The primary datapoint for IP, cybersecurity and consumer protection investigators in tackling infringing domain names, used to sell counterfeits and commit a wealth of other cyber-frauds misusing brand names, has been removed.

16. Some legal persons' data should be public – why should a user not know to whom they are giving their credit card details and other personal data? – and other registrant data should be rapidly disclosed on the basis of a legitimate request. Even though the EU's draft Network and Information Security Directive[5] is aimed at cybersecurity and not IP, AIM does hope that it will help to reset this balance, not least given the use of brand names in so many cybercrimes, such as phishing and other online frauds.

17. A common refrain when asking for any data is, "can't, GDPR". The GDPR does not apply to legal persons' data and neither was it intended to act as a shield for criminal activity. There should be no bar to online (or offline) intermediaries sharing legal persons' data with EU LEAs, and similar exchanges should be possible in other jurisdictions. Official guidance on the sharing of personal data necessary for IP crime investigations and consequent legal action is sorely needed and permitting an investigator to join the data dots pertaining to named individuals responsible for illegal activity should not be contentious.

18. Much of the above does not require legislation. Conversely, experience dictates that voluntary measures alone do not suffice. The EU's Digital Services Act (DSA)[6] does bring in some helpful measures, but as it is horizontal, applying to all forms of illegal content online and not only to goods, it is not future-proof when seen through the lens of the fight against counterfeiting.

19. Brand owners welcome the DSA's provisions that will help curb the sale of illegal goods online, including a harmonized EU notice-and-action mechanism to flag and remove online offers of illegal goods and additional obligations for very large platforms such as risk mitigation measures. However, AIM regrets that these new obligations do not apply to all online intermediaries involved in the sale and/or promotion of illegal goods online, notably social media, mobile applications and advertising platforms, as well as the failure to introduce a stay-down obligation on hosting service

---

[5] For more information on the Directive, see: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

[6] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

providers to prevent previously flagged and taken down/deactivated or similar content from reappearing on their services. AIM hopes that the forthcoming *EU Toolbox Against Counterfeiting*[7] will provide for practical tools and measures to close these loopholes.

IV. THE WAY FORWARD

20. The fight against counterfeiting is not just about protecting private rights. Due to IP crime's proven links with organized crime, the EU Agency for Law Enforcement Cooperation (Europol), supported by the European Union Intellectual Property Office (EUIPO), created the IP Crime Co-ordination Coalition. This has been reinforced by the reinstatement of IP crime as a priority under the European Multidisciplinary Platform Against Criminal Threats (EMPACT) for the period 2022 to 2025[8]. Studies and evidence from public bodies, including the Organization for Economic Co-operation and Development (OECD) and the EUIPO's European Observatory on Infringements of IP Rights consistently highlight consumer harm, including physical harm, caused by trade in counterfeit goods. Government revenue in the form of taxes and duties is depleted. Jobs are lost. Companies are bankrupted. Our very environment is endangered with the production and transportation of goods that should never have been made and cannot be sustainably destroyed or recycled as we do not know their raw materials.

21. This is a joint fight in which online intermediaries have a crucial role to play as long as their infrastructure and services are abused by criminals more interested in illegal gains than respecting laws, standards and safety. None of us, on- or offline, can do this alone. The politics of division have no place here. We must work together.

[End of contribution]

7 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12915-EU-toolbox-against-counterfeiting_en.

8 https://www.europol.europa.eu/crime-areas-and-statistics/empact.

THE PERSPECTIVE OF THE RECORDED MUSIC INDUSTRY ON THE ROLE OF ONLINE INTERMEDIARIES IN THE FIGHT AGAINST PIRACY

Contribution prepared by Mr. Lauri Rechardt, Chief Legal Officer, International Federation of the Phonographic Industry (IFPI), London, United Kingdom[*]

ABSTRACT

Online piracy remains a significant threat to the music industry. The International Federation of the Phonographic Industry's (IFPI's) Music Consumer Study 2021, the largest music-focused consumer study worldwide[1], found that 30 per cent of respondents used unauthorized sources to listen to or obtain music. This figure rose to 38 per cent amongst 16 to 24-year-olds.

Stream ripping – whereby content licensed only for streaming is copied or "ripped", and permanent digital copies are made of the streamed content – remains a major concern given the vast quantity of content made available.

Pre-release piracy – that is, the unauthorized making available of recordings before their release date – is another activity that is particularly harmful for right holders in the music industry given the negative commercial impact on legitimate sales. Pre-release content is often made available through social media platforms, while the actual content is stored on so-called cyberlockers. Cyberlockers usually do not require, let alone verify, identification information from their users, which makes it difficult for right holders to take direct action against the primary infringer(s).

Online intermediaries, the services of which are used by infringing online services, play a central role in addressing unauthorized uses effectively. This document will identify key measures and procedures that diligent online intermediaries should adopt and that would improve the enforcement of rights online.

These actions include clarifying the scope and conditions of the "safe harbour" liability privileges, implementing robust "know your business customer" (KYBC) policies, improving transparency and introducing robust repeat infringer policies.

IFPI also supports the further development of the WIPO ALERT Database as a trusted hub for collecting and sharing information on sites of concern provided by authorities in WIPO Member States for the benefit of the advertising industry.

I. A THRIVING MUSIC MARKET BUT ONLINE PIRACY REMAINS A CONCERN

1. The International Federation of the Phonographic Industry (IFPI) is the international trade association that promotes the interests of the recording industry worldwide. Membership across IFPI and its network of affiliated industry associations comprises 8,000 major and independent record companies in over 70 countries, which create, manufacture and distribute sound recordings.

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

[1] The study was conducted in 21 countries gathering the views of 43,000 respondents.

2. The music industry was one of the first to respond to the digital challenge. Prior to returning to growth in 2015, the industry experienced over 15 years of significant revenue decline, mostly due to the large-scale unauthorized use of music online. Throughout that difficult period, record companies continued to invest in artists, global systems and infrastructure, which enabled them to license over 60 million tracks and hundreds of digital services across the globe. Consequently, music fans today enjoy almost unlimited access to unprecedented amounts of diverse music, while artists have access to global markets and the opportunity to connect with fans across the world.

3. However, unauthorized uses of music online remain a serious problem for the recording industry, with the biggest concern being stream-ripping services, which enable users to make permanent copies of recordings from online streaming services. Recently, infringements have migrated from web-based services to mobile apps. IFPI estimates that 515 million tracks are downloaded from stream-ripping sites each month[2]. Cyberlocker services constitute a similar concern for right holders as they allow users to upload and distribute digital files on a dedicated storage infrastructure that is controlled, managed and maintained by the website operator. These services are often responsible for the distribution of pre-release content, which is particularly harmful for right holders' businesses. Other services of concern include certain social media platforms, online forums and messaging services used to share copyright infringing material at scale.

II. DUTY OF CARE AND RESPONSIBILITIES FOR ONLINE INTERMEDIARIES

4. Intermediaries of various types play a crucial role in the fight against online infringements. Due to their central role in the digital network environment, they are often best placed to prevent infringing activities.

5. Internet access providers, content delivery networks (e.g., Cloudflare), hosting service providers, search engines, domain registrars and registries, app stores, e-commerce marketplaces, payment providers and advertisers can all contribute to making the Internet a safer place and improving the functioning of the digital content market.

6. Legislators have acknowledged the need to strengthen the responsibilities and accountability of online intermediaries, as the recent United Kingdom Online Safety Bill[3] and the European Union (EU) proposal for the Digital Services Act[4] demonstrate. The form and scope of the measures that intermediaries can be expected to take may depend on the activity of the relevant intermediary. The following section outlines several reasonable and effective measures that would assist in making the Internet safer while creating a sustainable digital content market.

A. PROACTIVE MEASURES TO PREVENT COPYRIGHT INFRINGEMENTS

7. Hosting services, such as online platforms that store content uploaded by their users, play an increasingly important role in the online distribution of content.

8. In many jurisdictions, providers of such hosting services enjoy limitations from liability, also known as "safe harbors", provided they expeditiously remove infringing content upon gaining actual or constructive knowledge of it. However, with the evolution of the online ecosystem (web 2.0), these safe harbor provisions have, in many instances, become problematic. First, it is unclear

---

2 IFPI gathers data on visits to stream ripping sites from Similarweb and calculates the proportion of those visits which result in the successful download of copyrighted music content.

3 https://bills.parliament.uk/bills/3137/publications.

4 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.[5] https://www.copyright.gov/policy/section512/section-512-full-report.pdf.

which kind of platforms qualify for these privileges. Second, given the volume of content and the speed with which content is uploaded to these platforms, simple “take-down” measures have proven to be ineffective as the same content can be re-uploaded to the same service immediately afterwards.

9. Regarding the first point, EU legislators and the Court of Justice of the EU have sought to clarify the scope of the applicable safe harbor provisions. Essentially, the safe harbor provisions are limited to technical, automatic and passive intermediaries. Similarly, in its 2020 report on Section 512 of Title 17 of the United States (US) Copyright Act regarding safe harbors, the US Copyright Office questioned the application of safe harbor provisions to services that do more than merely store the content[5].

10. Concerning the second point, according to IFPI data, a large number of infringement notices sent by IFPI related to the same content and the same site. For example, in the case of Twitter in 2020, The Weeknd's *Blinding Lights* was notified over 3,700 times and Harry Styles' *Watermelon Sugar* was notified over 2,900 times after the first notice. This shows that the current “notice and take down” system has become an ineffective tool to address the sheer volume of copyright-infringing content online.

11. To address that issue, hosting service providers should ensure “stay-down” measures to be eligible for the safe harbor privileges. This means that upon becoming aware of an infringement, a hosting service provider must (i) remove all copies of the same work/sound recording and (ii) ensure the same work or recording (or copy thereof) is not re-posted or re-uploaded in the future (i.e., stay-down obligation), or risk facing liability.

12. “Notice and stay down” measures are an effective and proportionate obligation, also considering that such measures can be implemented through commercially available technologies, such as automatic content recognition applications.

B. REPEAT INFRINGER POLICIES

13. All intermediaries should also implement effective repeat infringer policies. This entails that where an intermediary knows or becomes aware that a recipient of its services (whether a reseller or end user) has repeatedly used its services to infringe intellectual property (IP) rights, the intermediary must (in appropriate circumstances) terminate the provision of its services to that recipient. Such an obligation is already part of the safe harbor conditions under the US Copyright Act.

14. The repeat infringer policy should be applied to prevent and deter the use of intermediaries’ services in connection with repeated and systematic illegal activities. The policy should also ensure that repeat infringers for whom the provision of services has been terminated are not permitted to use the service under a different name. To put such a policy into practice, it must be accompanied by an effective “know your business customer” (KYBC) policy[6].

15. Online intermediaries’ terms of service should set out in a clear and transparent manner the intermediaries’ right and discretion to suspend and terminate the provision of their services to repeat infringers in accordance with the principles set out above.

---

5 https://www.copyright.gov/policy/section512/section-512-full-report.pdf.

6 See below section IV.

III. TRANSPARENCY AND ACCESS TO INFORMATION

16. Lack of transparency, particularly the ease with which operators of illegal online services can hide their identities, is one of the most significant hurdles to the effective enforcement of IP rights online. Currently, operators can act in complete anonymity, protected by domain privacy services or shell companies, while intermediaries often fail to require their customers to provide proof of their true identities and correct contact details. This seriously undermines online enforcement efforts, including attempts to contact or bring action against the suspected infringers.

17. Governments around the world should consider a number of measures when addressing the lack of transparency online.

A. KNOW YOUR BUSINESS CUSTOMER AND RULES ON ACCESS

18. Legislation should require online intermediaries to implement effective KYBC policies, meaning that intermediaries should ensure they have accurate information about their business customers, including their contact details. Such obligations already exist in certain other sectors including the in financial/banking and legal services sectors. Further, the Digital Service Act, legislation, which is currently being finalized at EU level, proposes to include an obligation on online marketplaces to verify the identities of traders doing business on their platforms. The notion of a “business customer” should be interpreted to cover legal and natural persons acting in pursuit of direct or indirect gain. There should be appropriate penalties for failure to comply with the obligation and intermediaries should terminate services to business customers that fail to provide correct information. This obligation should also apply to any reseller of the original intermediary’s services.

19. In addition to a KYBC obligation, there should be a clear legal basis for persons with a legitimate interest in accessing information held by the intermediaries to do so in a timely manner. Right holders investigating infringements of IP rights, in accordance with the applicable law, have such a legitimate interest and should therefore be allowed access to that information.

B. PUBLICATION OF ACCURATE CONTACT DETAILS

20. There should be a general requirement for all information society services to publish accurate contact and operator details on websites. For instance, in the EU, Article 5 of the E-Commerce Directive[7] places such an obligation on Internet service providers. Unfortunately, in practice, enforcement of that obligation by the authorities of EU Member States has so far been lacking and there are few deterrent sanctions in the case of non-compliance. Robust transparency provisions of this kind and their effective enforcement are important, not only for IP right holders but more generally for consumer protection.

[7] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031.

C. ACCESS TO REGISTERS SUCH AS WHOIS

21. Following changes in data protection rules in Europe, the Internet Cooperation for Assigned Names and Numbers (ICANN)[8] introduced a Temporary Specification for WHOIS[9], which required registrars and registries to redact the vast majority of WHOIS data pertaining to European domain registrants (irrespective of whether they were natural or legal persons). The result has been an almost total, and often unjustified, withdrawal of the public WHOIS register, which far exceeds any requirements set forth in the EU General Data Protection Regulation (GDPR)[10] (which has been used to justify the withdrawal of access to WHOIS) and has significantly impacted the ability of right holders to obtain data necessary for the effective enforcement of their rights. Intervention is urgently needed to restore right holders' access to the WHOIS registry for the legitimate purpose of investigating and enforcing their IP rights. While there have been some legislative efforts to resolve the problem of inaccessibility to WHOIS information, such as the NIS2 Directive proposal[11] in the EU, these have thus far proven inadequate. Comprehensive intervention is urgently needed to clarify the public interest in a public WHOIS registry for right holders so that they can investigate and enforce their rights.

IV. ADDRESSING CROSS BORDER PIRACY

22. Services making money on the back of the unauthorized online distribution of music can establish themselves almost anywhere, and online copyright infringements can occur simultaneously across borders in any number of territories. Yet, when trying to stop the operations of these illegal businesses – whether by taking direct action against infringers or by seeking injunctions against the intermediary services used by the infringers – right holders need to take legal action in every single jurisdiction where the service is available. This makes addressing online infringements slow and prohibitively expensive and limits the effectiveness of any action taken by right holders to protect their rights.

23. For example, for over 15 years, right holders have been trying to stop IP infringements on the notorious website The Pirate Bay. The site's operators have faced civil and criminal litigation and cases have been referred to the Court of Justice of the EU as well as to the European Court of Human Rights[12]. All instances confirmed the copyright-infringing nature of the service, yet the site remains accessible in many jurisdictions around the world.

24. Legislators could do more to facilitate and improve the cross-border enforcement of IP rights. Substantive rights, enforcement measures and procedures are harmonized to a significant degree internationally by virtue of the World Intellectual Property Organization (WIPO) Internet Treaties and the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights. In appropriate cases, these commonalities should allow national courts to accept findings by competent judicial or administrative authorities in other countries as sufficient proof of claims of the same kind (e.g., claims regarding the infringing nature of a website). This could be important, for example, in cases involving no-fault blocking injunctions against online intermediaries which relate to the same service operating in several jurisdictions, as well as direct infringement cases

---

8 ICANN is a multi-stakeholder group that coordinates several databases relating to the Internet.

9 WHOIS is a protocol that links to databases kept by domain registrars and registries in relation to information of their customers.

10 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj9.

11 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN.

12 C-610/15 *Stichting Brein v **Ziggo** BV and XS4ALL Internet BV* (2017) available at: https://curia.europa.eu/juris/liste.jsf?language=en&T,F&num=c-610-15; *Neij and Sunde Kolmisoppi v Sweden* (2013) Application no. 40397/12, available at: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2240397/12%22]}.

involving the same content, the same right owners and the same online service operating across territories. Furthermore, courts should have the power to assess damages on a global basis and they should not be limited to the territory of their jurisdiction.

25. In this context, IFPI supports the efforts of WIPO to promote the WIPO ALERT Database. IFPI believes this initiative can play a crucial role in collecting and sharing information on sites of concern provided by authorities in WIPO Member States for the benefit of the advertising industry. Governments should also encourage and facilitate local dialogue between right holders and intermediaries to agree on voluntary solutions, similar to the codes of conduct on website blocking agreed by stakeholders in Germany[13], Portugal[14], Denmark[15], Spain[16], the Netherlands[17] and Sweden[18], or the memoranda of understanding agreed upon between advertisers, advertising intermediaries and right holders.

[End of contribution]

13 https://cuii.info/ueber-uns/.
14 https://edri.org/our-work/portugal-voluntary-agreement-against-copyright-infringements/.
15 https://rettighedsalliancen.com/new-code-of-conduct-agreement-between-the-telecommunications-industry-and-the-rights-alliance-ensures-more-effective-enforcement/ and https://rettighedsalliancen.com/wp-content/uploads/2020/11/CoC_ENG.eksl_.Anneks.pdf.
16 https://www.culturaydeporte.gob.es/actualidad/2022/01/220121-protocolo-antipirateria.html
17 https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content.
18 https://rattighetsalliansen.se/wp-content/uploads/2022/05/Branschoverenskommelse.pdf.

TACKLING CUSTOMS COMPLIANCE IN THE EXPRESS INDUSTRY – THE APPROACH OF DHL EXPRESS

Contribution prepared by Ms. Sandra Fischer, Global Customs Head; Ms. Asha Menon, Vice President, Global Customs Compliance and Regulatory Affairs; Mr. Marcelo Godoy Rigobello, Vice President, Global Customs Customer Support; and Gordon Wright, Vice President, Customs and Regulatory Affairs EU, DHL Express, Diegem, Belgium[*]

ABSTRACT

In a world that has become more interconnected than previous generations could have ever imagined, global trade has never been more important. The rapid growth of e-commerce and the COVID-19 pandemic have significantly increased the number of international parcels moving across the world, resulting in more challenges from a customs and trade compliance perspective. This document provides a high-level overview of the DHL Express' approach to ensuring customs compliance in its network, as well as proposed areas of cooperation with authorities to tackle non-compliance.

I. DHL EXPRESS' CUSTOMS COMPLIANCE APPROACH

1. DHL Express is fully committed to compliant trade. Customs compliance is a core element of the DHL Express culture and value proposition to its customers together with its ethical working remit. The DHL Express Customs Compliance Team's mission is to enable sustainable business growth, by providing a compliant and efficient cross-border trade experience to its customers through collaboration with Authorities.

2. For many years, DHL Express has had in place a series of pro-active checks to prevent non-compliant shipments from entering its global network. Examples include:

- physical security screening of air freight shipments prior to departure of airplanes (e.g., via X-ray inspections);
- physical shipment inspections/examinations (e.g., to pro-actively identify non-declared dangerous goods); and
- denied party screening of all shipments using data analytics (based on the consignor and consignee information).

3. In addition to these pro-active checks, DHL Express is now launching the Global Customs Compliance Program with the goal of improving even further the shipment integrity and commercial invoice data quality provided by shippers. This will allow customs authorities to carry out a more targeted risk assessment and support compliant customs clearance processes.

4. In order to make the internal compliance initiatives successful, DHL Express believes that strong collaboration with customs authorities is required to educate the shippers. It is essential that customs authorities enhance direct communication with the shippers (i.e., the party that actually provides the physical goods and data/information) regarding the importance of providing

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

high-quality data when shipping internationally, and make them fully aware of their responsibilities when shipping across borders.

II. DHL EXPRESS' GLOBAL CUSTOMS COMPLIANCE PROGRAM

5. DHL Express is launching the Global Customs Compliance Program to further increase the focus on educating its customers in the following four risk areas:

- intellectual property rights (IPR): to prevent shippers from sending prohibited IPR infringing goods via DHL Express;
- undervaluation (UV): to prevent shippers from under-declaring the value of goods on the commercial invoice in order to pay less (or zero) duties/taxes;
- goods descriptions (GD): to prevent shippers from providing incomplete/inaccurate descriptions of goods to bypass security screening; and
- true shipper and receiver (TSR): to prevent shippers from providing inaccurate shipper/receiver information to bypass security/denied party screening.

6. The key theme running through the four risk areas above is data quality. Therefore, as DHL Express pro-actively continues to engage with its customers to educate and raise awareness on the importance of providing complete and accurate data to safeguard legitimate goods when shipping with DHL Express, it is critically important to make shippers aware that non-compliance has serious and tangible consequences.

7. In addition to educating its customers, DHL Express is also further educating its own employees via internal communications and trainings, and enhancing its internal risk management mitigation processes and tools in order to reduce the probability of non-compliant shipments entering the DHL Express network. The internal initiatives include, *inter alia*:

- enhancing new account opening measures, to avoid on-boarding known offenders;
- piloting data analytics and machine learning tools, to pro-actively identify and intercept potential non-compliant shipments in origin countries; and
- enhancing shipment booking systems to guide shippers on how to create complete and accurate goods descriptions when shipping with DHL Express.

Image 1: Examples of DHL Express internal posters to further increase awareness of the employees regarding four non-compliance customs risk areas.

III. PROACTIVE ADDRESSING OF INTELLECTUAL PROPERTY INFRINGEMENTS IN PRACTICE

8. DHL Express Hong Kong has a dedicated team that pro-actively inspects goods on a daily basis, and works closely with the Hong Kong Customs Authorities targeting IPR infringing goods. During 2020 and 2021, DHL Express Hong Kong physically intercepted over 28,000 outbound shipments to identify suspected IPR infringing goods.

Image 2: DHL Express Hong Kong employees performing physical inspections of suspected IPR infringing goods.

9. In October 2021, in a "Letter of Appreciation", Hong Kong Customs Authorities praised DHL Express Hong Kong for its efforts in the field of anti-smuggling resulting in a seizure of IPR infringing goods and other illicit commodities valued at HKD 7.6 million during the third quarter of 2021. This demonstrates the continued commitment of the DHL Express Hong Kong team towards compliant trade.

10. DHL Express USA, in close collaboration with U.S. Customs and Border Protection (CBP), works to proactively intercept and inspect suspected IPR infringing goods, and operationally supports the IPR voluntary abandonment program[1]. DHL Express USA has dedicated resources to identify and remove IPR infringing goods from its network, and it collaborates with origin teams to eliminate "bad shippers" from its network. In 2021, the DHL Express USA team physically intercepted more than 3,500 shipments to identify suspected IPR infringing goods, together with CBP, contributing to many "bad shipper" account closures. Also in 2021, more than 5,000 shipments valued at USD 246.3 million were referred to CBP's IPR abandonment process, saving U.S. taxpayers more than USD 49 million[2].

11. CBP at the Port of Cincinnati has stated that their partnership with DHL is invaluable, and DHL's assistance with the enforcement of IPR infringing and prohibited goods is instrumental to the CBP mission. The National Intellectual Property Rights Coordination Center (IPR Center) presented DHL Express USA with an award for being the most active partner in the express delivery sector and working closely with the IPR Center to provide intelligence and operational support concerning counterfeit goods.

12. In order to ensure continued success in tackling IPR infringements, one potential area of further cooperation between regulatory authorities and express providers is to increase the exchange of intelligence regarding non-compliant targeted shippers. A coordinated effort across the end-to-end supply chain by all stakeholders could have a significant impact. IPR infringers are constantly adapting, selling, and moving non-compliant goods via different online marketplaces and social media platforms, different shipping routes, different transport providers, and different

---

[1] A pilot program where customs detain suspected IPR-infringing shipments and DHL presents the customer with the option to either abandon the goods or contest custom's IPR infringement findings. This process allows customs to quickly remove IPR-infringing shipments from the network without a lengthy seizure process.

[2] The figure is based on a US CBP article "Cincinnati CBP Breaks Records in Fiscal Year 2021", accessible here: https://www.cbp.gov/newsroom/local-media-release/cincinnati-cbp-breaks-records-fiscal-year-2021.

transport modes. Therefore, it is critical to ensure strong cooperation and effective information sharing between all stakeholders.

IV. DHL'S RECOMMENATION FOR REGULATORY AUTHORITIES

13. One concrete recommendation is that authorities (together with right holders) develop and maintain a central list of "IPR violators", which can be accessed by banks, social media, online selling platforms, and transport providers. This database would allow each of the stakeholders to prevent IPR violators from doing business, as a coordinated effort. Based on such a database, for example, DHL Express could flag IPR violators in their internal systems to prevent account opening, to trigger shipment intercepts, and to provide additional intelligence/information to relevant authorities (where legally allowed).

V. CHALLENGES

14. Despite the various ongoing efforts, there are still many challenges, which could be addressed jointly by industry and regulatory authorities concerned, such as:

- Not all local enforcement agencies are fully engaged in identifying or stopping IPR infringing goods through a joint approach with DHL Express.
- Not all rights holders follow procedures in place to initiate potential seizures of IPR infringing shipments through the enforcement agencies.
- With only limited information sharing from enforcement agencies, DHL Express is not able to further develop a targeted risk-based approach towards IPR infringement. Examples where collaboration could be improved to increase the success of joint efforts are:
  - seizures being communicated in a timely manner, on a regular basis and in a digital format for ease of further processing;
  - seizure information including details of commodities and variations versus shipper invoice; and
  - handling of IPR infringing goods that have been identified by DHL Express by the authorities. Currently it is up to the DHL to either destroy or return the shipment.
- X-ray screening does not assist in identifying IPR infringing goods. IPR inspection requires opening each shipment to check the contents to see if it contains any commodities with potential branding / copyright issues. This manual process involves additional resources and is very time consuming. Data sharing and market intelligence from regulatory authorities could reduce this manual effort.
- Shipments containing suspected IPR infringing goods have to be inspected by authorities and potentially seized. Storing these shipments pending results has a negative impact on the DHL's storage capabilities and quicker response times would reduce operational demands.
- DHL is not an enforcement agency, hence, does not have the intelligence nor the authority to stop shipments.

VI. CONCLUSION: BENEFITS OF PRO-ACTIVE COLLABORATION WITH REGULATORY AUTHORITIES FOR ALL PARTIES

15. Effective enforcement of non-compliant trade requires a risk-based and threat managed approach, as well as cooperation and information sharing between the various end-to-end supply-chain stakeholders, such as customs authorities and the express industry. Express operators cannot act as an enforcement agency, but can take appropriate action based on information shared by customs authorities to fight non-compliant behavior.

16. DHL Express is committed to compliant trade and continuously supports authorities across the world in tackling illicit trade by:

- cooperating and providing accurate and timely electronic shipment data for customs authorities to perform risk assessment of shipments as early in the process as possible;
- intercepting and handing over physical shipments flagged by customs authorities as non-compliant;
- acting against non-compliant shippers flagged by customs authorities; and
- providing additional support and information on major investigations by customs authorities (e.g. details on shippers and consignees, where legally allowed).

17. As outlined in this contribution, DHL Express is going above and beyond, and is fully engages in pro-actively tackling non-compliant areas by:

- cooperating with customs authorities;
- undertaking shipment checks at the point of origin, on both physical goods and shipment data quality;
- leveraging data analytics and machine learning to pro-actively identify non-compliance shipments;
- stopping suspected non-compliant shipments in the network; and
- closing down accounts of non-compliant shippers.

18. Therefore, it is important for DHL Express that authorities acknowledge and recognize the efforts being undertaken. DHL Express believes that such recognition is pertinent to them continuing going above and beyond, and that it is a win-win situation for customs administrations, other government agencies, the customers and DHL Express itself.

19. Lastly, it is essential that relevant authorities further develop and enhance direct communication with shippers regarding the importance of providing high-quality data when shipping internationally, and make shippers aware that non-compliance has serious and tangible consequences.

22. DHL Express is fully committed to compliant trade, and welcomes further cooperation efforts and pilot projects together with customs authorities, other government agencies and industry players to tackle illicit trade.

[End of contribution]

MASTERCARD'S INITIATIVES TO PREVENT INTELLECTUAL PROPERTY INFRINGEMENTS

Contribution prepared by Mr. Jonathan Trivelas, Vice President, Brand Performance Team, Customer Engagement and Performance, Mastercard International, Purchase, New York, United States of America[*]

ABSTRACT

Mastercard is committed to fighting intellectual property (IP) infringement and does not tolerate the use of its brand, network, programs, or services to further any illegal activity. It is important to note that Mastercard does not have a direct relationship with, and does not underwrite, Merchants that accept Mastercard cards for payment. Instead, the Merchant enters into a contract with a financial institution, referred to as an Acquirer, and it is the Acquirer that has the direct relationship with Mastercard as a licensed Customer. Mastercard Customers, their Merchants, and all other network participants are required to comply with all applicable laws, as well as the Mastercard Rules and other Standards.

Mastercard frequently cooperates and works closely with law enforcement, right holders, and other organizations on matters concerning alleged illegal activity, including intellectual property infringements. Mastercard also has several programs and tools to help Acquirers prevent illegal activity, such as the Mastercard Alert to Control High-risk (Merchants) (MATCH™) and the Merchant Monitoring Provider (MMP).

I. OVERVIEW OF MASTERCARD'S ROLE IN THE PAYMENTS ECOSYSTEM AND THE FOUR PARTY MODEL

1. Mastercard conducts various processing activities in different capacities. Mastercard's core activity is processing payment transactions on behalf of its Customers. This core activity typically involves four parties: Mastercard, financial institutions, Merchants, and the cardholder. The financial institutions issue Mastercard payment cards to their Customers, who are individuals or businesses (cardholders). The bank acting in this capacity is referred to as an 'Issuer' or 'Issuing bank'. A cardholder may then use its Mastercard card to make a payment to a Merchant (e.g., a brick-and-mortar or online store). A bank that facilitates the payment from a cardholder's Issuer to the Merchant is referred to as an 'Acquirer' or 'acquiring bank'.

2. The cardholder has a contractual relationship with their Issuer(s). The Merchant has a contractual relationship with their Acquirer(s). Both Issuers and Acquirers contract with Mastercard to enable payment transactions, as Mastercard Customers. Mastercard does not have a direct relationship with Merchants or cardholders.

3. A payment is facilitated by an Acquirer, who receives the payment request from a Merchant and sends it to the cardholder's Issuer via the Mastercard network. The Acquirer subsequently receives the payment from the Issuer via the Mastercard network and deposits it in the Merchant's bank account. A Merchant must contract with an Acquirer to be able to accept payments via a

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

Mastercard card and it is the Acquirer that is responsible for knowing their Merchant and monitoring their Merchant's activity.

4. Mastercard also establishes and maintains the Rules and Standards that govern all aspects of Mastercard activity, and one of its fundamental principles is legality. Mastercard does not tolerate the use of its brand, network, programs, or services to further any illegal activity. Mastercard Customers, Merchants, and other network participants are required to comply with all applicable laws and the Mastercard Rules and Standards. Mastercard has programs in place to detect illegal activity and requires immediate action should such be detected.

II. MASTERCARD'S EFFORTS TO COMBAT INTELLECTUAL PROPERTY INFRINGEMENTS

A. MASTERCARD'S ANTI-PIRACY POLICY

5. Mastercard's policy for addressing the online sale by a Merchant of copyright-infringing products and counterfeit trademark products (the "Anti-Piracy Policy")[1] supports, and is considered in conjunction with Mastercard's Business Risk Assessment and Mitigation ("BRAM") program. Under this policy, Mastercard accepts and investigates referrals from both law enforcement and non-law enforcement sources (i.e., right holders and their qualified representatives) relating to the online sale of a product or service that allegedly infringes copyright or trademark rights of another party.

B. THE BUSINESS RISK ASSESSMENT AND MITIGATION PROGRAM

6. The Business Risk Assessment and Mitigation (BRAM) program was established in 2005 to investigate and address Customers engaged in activity that is illegal. Mastercard may become aware of a potential violation through the referral from law enforcement agencies, right holders, or an internal investigation. The BRAM team investigates the alleged activity and may perform a "trace" transaction at the violating website to confirm the acceptance of Mastercard cards for payments at the site and determine the identity of the Acquirer, or Mastercard Customer, under which that Merchant is processing.

7. If the Merchant is identified as potentially noncompliant, the Acquirer for that Merchant is notified. The Acquirer must investigate the concern and report back to Mastercard with their findings and confirmation that all illegal activity has ceased. If the Acquirer determines that the Merchant was not engaging in illegal activity, the Acquirer must provide Mastercard with compelling evidence demonstrating that finding. If the Merchant is found to have engaged in illegal activity and is terminated by the Acquirer, the Acquirer must report the Merchant to MATCH (Mastercard Alert to Control High Risk). MATCH is a database of Merchants terminated by the Acquirer for violation of Mastercard Rules and Standards. At the conclusion of the investigation, Mastercard leverages noncompliance assessments to deter future instances of illegal activity and to enforce the message that there is zero tolerance for illegal activity within the Mastercard network.

[1] Accessible at: https://www.mastercard.us/en-us/vision/who-we-are/terms-of-use/anti-piracy-policy.html.

a) Transaction Laundering and Other Challenges

8. Transaction laundering (also called transaction factoring or factoring) is a common tactic used by Merchants engaged in illegal activity to evade detection by their Acquirer and Mastercard, and is prohibited under Mastercard Rules and Standards. Transaction laundering occurs when a Merchant routes payments for illegal activity through a Merchant account that was approved for a different website. The violating website, or the website processing payments for the illegal activity, is unknown to the Acquirer. For example, a Merchant will get approved for a Merchant account by the Acquirer to sell shoes via the website goodshoes.com. During the Merchant onboarding process, the Acquirer will review goodshoes.com to confirm that no illegal products or services are being offered and then allow the Merchant to process Mastercard cards for payments as a shoe store. However, the Merchant is also operating a site offering counterfeit luxury watches called fakewatches.com that is not disclosed or otherwise known to the Acquirer. When a cardholder makes a purchase at fakewatches.com, the transaction is routed (or “laundered”) via the Merchant account set up for goodshoes.com.

9. It is the Acquirers’ obligation to ensure that their Merchants are not engaged in transaction laundering. Mastercard recognizes it can be challenging to detect and mitigate this activity, but one effective effort has been a combination of robust due diligence practices, effective transaction and dispute monitoring, and the use of web crawling technology to monitor website content.

10. In addition, Mastercard is faced with the challenge of not being experts on intellectual property rights, nor the owners of the IP that is being infringed. Mastercard also does not have a direct relationship with the Merchant or any insights into their ownership or contractual relationships with other entities. As a result, Mastercard is often not able to confidently conclude that a Merchant is selling a product that violates IP without confirmation from the IP right holder or law enforcement.

b) Merchant Monitoring Program

11. There are several third-party Merchant Monitoring Service Providers (MMSPs) that help Acquirers monitor illegal activity, including signs of transaction laundering. Mastercard created the optional Merchant Monitoring Program (MMP). It encourages Acquirers to register their MMSP with Mastercard and submit monthly reports confirming which Merchant URLs are being monitored in order for credit against potential noncompliance assessments. If a Merchant being monitored as part of the MMP is subsequently identified by Mastercard as engaging in illegal activity and/or transaction laundering, and all of the requirements of the MMP have been met by the Acquirer, Mastercard may provide a partial mitigation to the applicable noncompliance assessments. The requirements include the following: the Acquirer must register the MMSP with Mastercard, the MMSP must persistently monitor the identified Merchant and the Acquirer/MMSP must submit monthly reports to Mastercard confirming such monitoring, the Acquirer must take prompt action upon notification of a BRAM identification and the Acquirer/MMSP must provide an incident report with regard to the identified Merchant.

c) Partnerships

12. Each year Mastercard addresses hundreds of cases of intellectual property rights (IPR) violations, where either the illegal content is removed from the Merchant’s website or the Merchant’s ability to accept Mastercard cards is terminated. The strength of the BRAM program is based on partnerships, as IPR violations are not always easily identifiable and often times require confirmation by the IP right holders themselves. Mastercard regularly engages with law enforcement agencies, such as the Royal Canadian Mounted Police and the City of London Police,

who validate consumer complaints and refer cases to Mastercard for action. Mastercard also regularly engages with industry groups, such as the International Anti-Counterfeiting Coalition (IACC) and the Motion Picture Association (MPA), who have right holders as members. Through these partnerships, participating brands can refer cases to Mastercard for investigation. In addition, right holders themselves can directly refer cases to Mastercard, as outlined in the Mastercard Anti-Piracy policy.

C. MATCH™

13. The Mastercard Alert to Control High-risk (Merchants) (MATCH™) system is designed to provide Acquirers with the opportunity to develop and review enhanced or incremental risk information before entering into a Merchant Agreement. MATCH is a tool that helps Acquirers evaluate potentially high-risk Merchants – or those who have had Rules and Standards violations – during due diligence and before beginning any work with them, and it is mandatory for Acquirers licensed by Mastercard, unless prohibited by local law. When an Acquirer considers signing a Merchant to accept Mastercard cards for payment, MATCH can help the Acquirer identify whether the Merchant was terminated by another Acquirer due to circumstances that meet the MATCH Add criteria. MATCH Add criteria are a list of reasons for adding a merchant to MATCH when an Acquirer terminates that Merchant for a violation of Mastercard Rules and Standards. For example, if a Merchant is found to have processed illegal transactions, that would meet the criteria for requiring the Acquirer to add the Merchant to MATCH using the designated reason code. Each reason code specifically designates why the Merchant was added to MATCH so that any subsequent Acquirer will have knowledge of that prior activity. This information could impact the Acquirer's decision whether to acquire for this Merchant and/or whether to implement specific action or conditions to monitor and mitigate potential risk. However, it is important to note that MATCH is not a blacklist, as Acquirers are not prohibited from onboarding a Merchant listed in MATCH.

III. CONCLUSION

14. Mastercard is committed to fighting IP infringement and providing a safe, smart, and secure global payments network. Mastercard believes that information sharing partnerships with right holder groups, payment networks, law enforcement and government agencies that work together to identify violations and terminate the acceptance of Mastercard cards and other payment mechanisms is critical to the fight against IPR violations. Disrupting the flow of funds to bad actors is the key to ending this illegal activity. Mastercard looks forward to continuing the discussion on IP infringement prevention, detection and mitigation, and how further partnerships can be built in this space.

[End of document]