EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

PAYMENT – DISCUSSION PAPER

Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities

November 2021

DISCLAIMER

The views expressed in this discussion paper do not represent the official position of the EUIPO. This paper is based on the work of the EUIPO Observatory's Expert Group on Cooperation with Intermediaries. The views expressed in this discussion paper cannot be attributed to the Expert Group as a whole or to any single contributing expert.

The Observatory welcomes any further input or comments on this discussion paper in order to continue deepening its understanding of good practices in undermining the misuse of electronic payment services for intellectual property-infringing activities. This discussion paper may be subject to reviews or updates based on any further input from experts or new developments in the field.

ISBN 978-92-9156-305-0 doi: 10.2814/346710 TB-07-21-076-EN-N

Foreword

The Expert Group on Cooperation with Intermediaries was set up to further the understanding of different intermediary services, how they can be misused for intellectual property infringing activities, and how these misuses can be counteracted through good practices. Having looked at domain names([1]) and social media([2]), this third discussion paper examines payment. It will hopefully contribute to a better understanding of:

- how electronic payment services are misused to infringe intellectual property (IP) or support IP-infringing activities;
- the challenges raised by such misuses;
- the existing and developing good practices through which these challenges can be met.

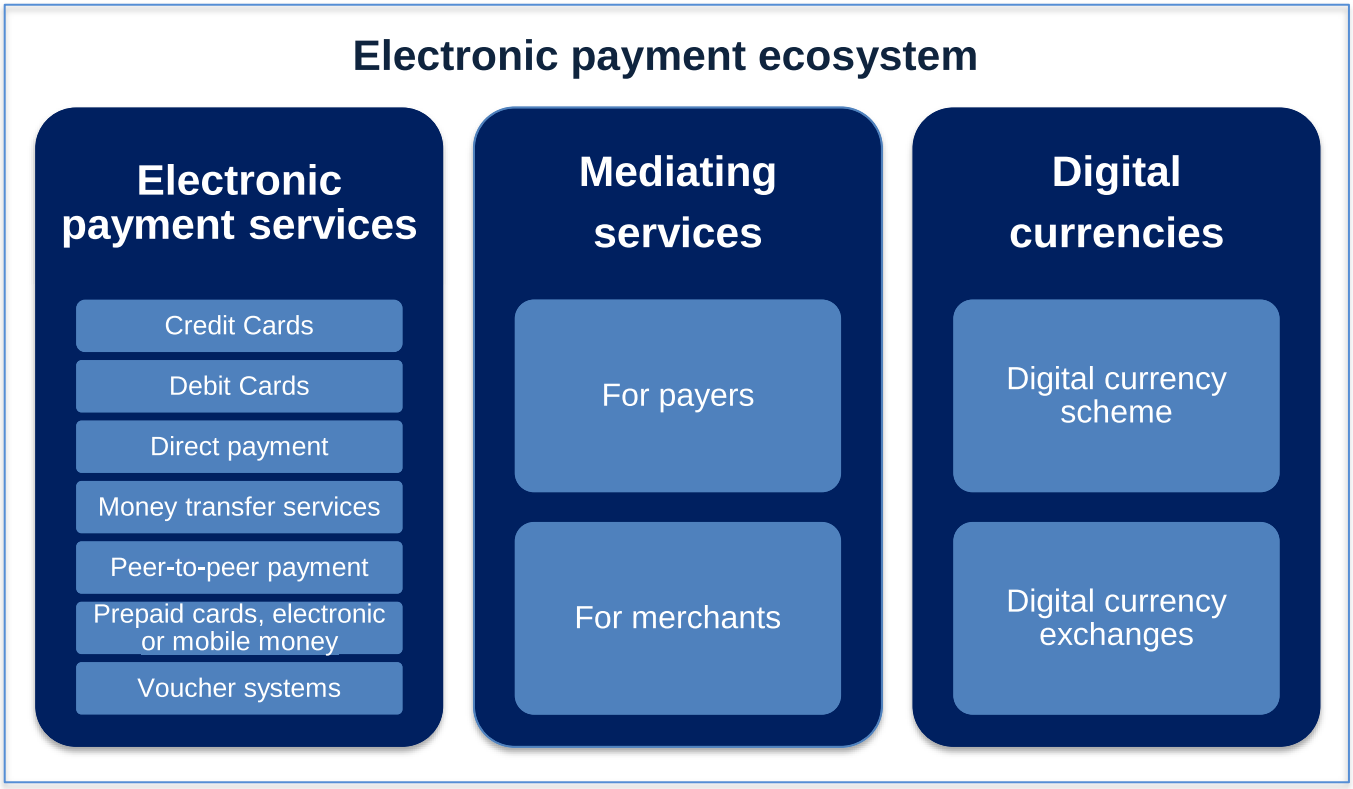
([1]) EUIPO, Domain names – Discussion paper: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP-infringement activities, March 2021.

([2]) EUIPO, Social Media – Discussion paper: New and existing trends in using social media for IP-infringement activities and good practices to address them, June 2021.

Table of Contents

Executive Summary

The electronic payment ecosystem is complex and changing fast. In addition to the different payment cards, the development of internet and mobile payments, digital money transfers and electronic currencies gives rise to new services and new types of payment intermediaries.



Intellectual property-right infringers engaging in the sale of counterfeit goods or providing services for pirated content depend on various payment services for their activities. They increasingly engaged in sophisticated uses of different payment services to undermine the investigative measures used to establish the illegal nature of their activities, and to make the flow of funds more complicated to trace.

In the context of this discussion paper, experts identified a number of emerging trends and challenges that electronic payment service providers, intellectual property (IP) owners and law enforcement authorities are facing in counteracting the misuse of payment services for IP-infringing activities including:

- **transaction laundering**, which consists of directing payments for illegal transactions through a legitimate, or legitimate appearing website, with or without knowledge of the merchant responsible for the website and the associated card account; transaction laundering can be difficult to detect and is counteracted through sophisticated monitoring of transactions and websites to detect illegal activities;

- the **identification of IP infringers across different payment services, as well as other intermediary services**, such as e-commerce marketplaces that provide IP infringers with access to different payment options;

- the **sharing of information,** which was identified as an overarching challenge, in particular with regard to the information about IP infringers that can be shared with law enforcement authorities or between private players; experts stressed the need for guidance on what information can be shared in line with European Union (EU) data protection and competition laws.

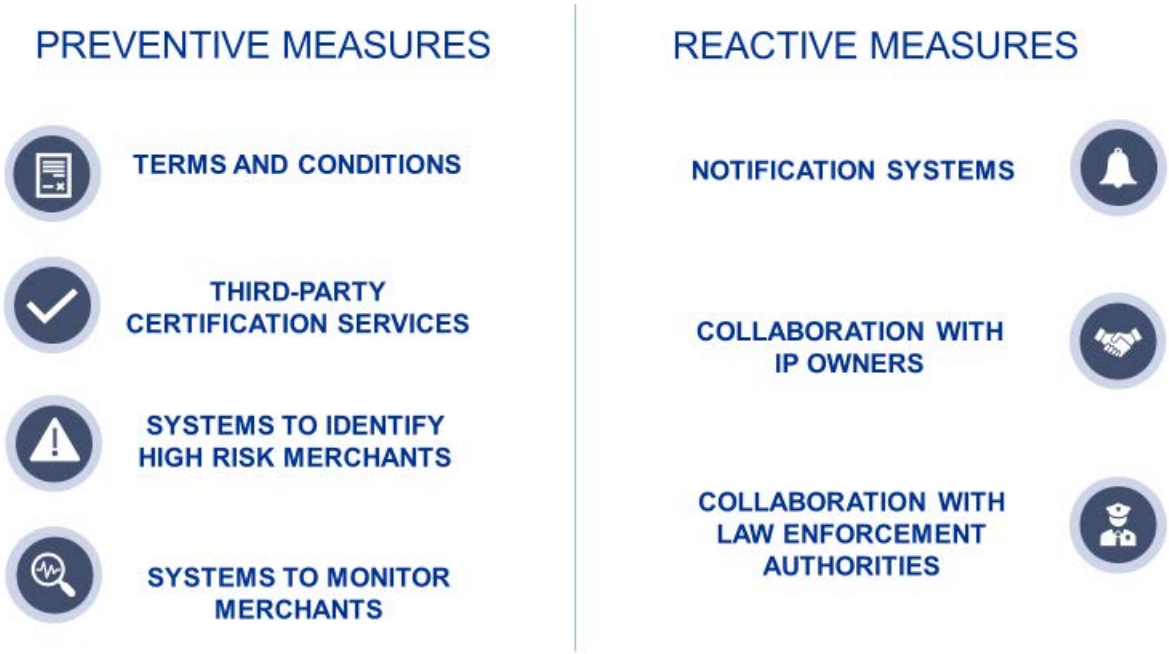
Unlike other types of intermediaries, payment service providers are subject to strict regulatory requirements to deal with fraud and illegal activities, and in particular money laundering. This includes:

- **customers due diligence requirements**, which vary on a risk-based approach;

- **internal controls and monitoring systems** of the customers' activities, which also vary on a risk-based approach;

- **reporting of suspicious activities** to the national Financial Intelligence Unit (FIU).

The different levels of due diligence and related obligations to onboard customers and/or monitor their activities are reflected in a number of **good practices** developed by some payment services that are seeking ways to limit the risks of their services being misused for IP-infringing activities.



The experts identified a number of good practices in place to pre-empt the misuse of payment services. These are, in particular, the following.

- **Terms and conditions** clearly prohibiting activities infringing, or facilitating the infringement of IP rights, or qualifying certain activities as high risk (e.g. cyberlockers) and requiring enhanced due diligence review and/or monitoring obligations.

- **Third-party certification** for online pharmacies to ensure that their activities effectively comply with all applicable laws.

- **Systems to identify high-risk merchants** across different payment services, with the setting up of databases of merchants that have been terminated due to a high number of user requests for a refund, or for violation of a payment service provider's terms and conditions. These systems contribute to identifying high-risk merchants, including repeat IP infringers.

- **Systems to monitor merchants' activities**, including through dedicated service providers, which use a range of techniques to detect online illegal activities or the sale of restricted goods.

The experts identified other good practices to deal with the actual misuse of payment services in the context of IP-infringing activities. These are, in particular, the following.

- **Notification systems** put in place by some payment services for IP owners to report suspected IP-infringing activities using their services.

- **Collaboration with IP owners**, supporting the sharing of lists of websites that have been ruled illegal by courts, or facilitating the reporting of online sellers of counterfeit goods.

- **Collaboration with law enforcement authorities** that support the refunding to consumers that have mistakenly bought counterfeit goods, or specific enforcement operations targeting IP infringers and IP-infringing services. On this last point, experts pointed to ongoing collaborations related to other types of illegal activities that could be used or replicated to counteract IP-infringing activities.

Payment service providers are in a unique position to identify IP infringers and stop payments related to IP-infringing activities. This discussion paper will hopefully contribute to further the understanding of the existing and developing good practices in that field, and of the opportunities to extend or replicate some of them.

1 Introduction and background

The use of cash and bank cheques has dropped over the years in most developed countries, with businesses and consumers increasingly relying on electronic payment systems. 'With nearly 70 billion payments in 2017, payment cards are the most widely used electronic payment instrument in the European Union (EU), already totalling more than half (52 %) of all non-cash transactions, with credit transfers accounting for 24 % and direct debits for 19 %' ([3]). At the same time, a number of new electronic payment options are emerging, together with digital currencies and cryptocurrencies, all involving non-traditional payment intermediaries.

IP right infringers that sell counterfeit goods, or provide services for pirated content, depend on various payment services for their activities.

> [They] often use financial services provided through sales platforms, especially online payment systems. Although online payment systems have been used for a long time, the way counterfeiters are using them is becoming more sophisticated. Money is often transferred to other accounts outside the EU, thereby crossing jurisdictions and making it considerably more complicated to trace. Sellers of counterfeit goods frequently maintain online payment accounts that are only used once or twice, thereby hiding the scale of their activities ([4]).

Some IP infringers also use measures and technologies to avoid detection and undermine investigative measures used to establish the illegal nature of their activities and subsequently to block their access to payment services ([5]) ([6]).

The terms and conditions of electronic payment services generally include rules prohibiting the misuse of their services, provide a 'complaint system' and, in some cases, refund money paid for counterfeits. However, their services continue to be exploited for Business-to-Consumers and

([3]) European Central Bank - Card payments in Europe – current landscape and future prospects: a Eurosystem perspective, April 2019.

([4]) Europol and EUIPO 'Intellectual Property Crime Threat Assessment 2019', p. 37.

([5]) IACC - 'Payment Processor Portal Program: First Year Statistical Review', October 2012, p. 1.

([6]) Some payment service providers are also rights holders and one of the most repeated infringement of their rights is the use of card scheme logos on IP-infringing websites to make them appear legitimate.

Business-to-Business IP-infringing business models. This raises concerns with IP owners and law enforcement authorities regarding the increasingly sophisticated use of payment services, including laundering the proceeds from IP-infringing activities([7]).

Cooperation with payment services is central to preventing or terminating this use and to being able to follow the flow of funds to identify IP infringers. As announced in the package of measures on the protection of intellectual property rights (IPRs) adopted in November 2017([8]), the European Commission reaffirmed its commitment to working on a 'follow the money' approach and supporting 'industry-led initiatives to combat IP infringement', notably in the field of payment.

In this context, the EUIPO Observatory on infringements of IP rights (the Observatory) asked its Expert Group on 'Cooperation with intermediaries'([9]) for help in furthering the understanding of the different uses of payment services for IP-infringing activities, and of good practices that counteract this use.

This analysis is based on discussions with the Expert Group with the aim of:

- listing the different electronic payment services and their misuses in the context of IP-infringing activities (Section 2);
- better understanding the regulatory requirements applying to payment services and how they support the development of good practices (Section 3);
- identifying some of the challenges to prevent the misuse of payment services for IP-infringing activities (Section 4);
- identifying good practices to counteract these activities (Section 5).

([7]) Europol and the EUIPO 'Intellectual Property Crime Threat Assessment 2019', p. 39.

([8]) See European Commission Communication on 'A balanced IP enforcement system responding to today's societal challenge', November 2017.

([9]) The EUIPO Observatory Expert Groups help and guide the implementation of Observatory projects in focused and specialised areas, in this case the 'Cooperation with intermediaries'. Experts are called upon to provide expert support to the Observatory's agreed projects and activities. Experts represent themselves and not a particular organisation nor institution.

2 Electronic payment services

The electronic payment ecosystem is complex and changing fast. These changes are driven by technological developments, as well as 'enabling regulations'([10]), such as the revision of the Payment Service Directive([11]), that supports the development of innovative services in the EU. In addition to the different payment cards, the development of internet and mobile payments, digital money transfers and electronic currencies gives rise to new services and new types of payment intermediaries.

2.1 Electronic payment services and intermediaries

There is no agreed classification of electronic payment services and no consistent terminology to describe them. As a first step to furthering the understanding of the payment ecosystem, this analysis has identified a number of services and intermediaries that:

- allow electronic payments (Section 2.1.1);
- facilitate the use of these services (Section 2.1.2); or
- provide for the use of new digital currencies (Section 2.1.3).

2.1.1 Electronic payment services

- **Credit cards**: enable cardholders to make purchases and/or withdraw cash up to a prearranged credit limit. The credit granted is settled in full by the end of a specified period, or in part, with the balance taken as extended credit. In both cases, this means that the funds for individual transactions are not deducted immediately from the cardholders' accounts, leaving them time to dispute wrongful or fraudulent payments.

([10]) BCG and Google, Digital Payments 2020, July 2016, p. 8.

([11]) Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market and corrigendum to Directive (EU) 2015/2366.

Credit card companies can be divided into two different categories depending on their business relationship with the merchants that accept cardholders' payments. In **closed-loop networks**, payment processors have a direct contractual relationship with merchants (e.g. American Express). In **open-loop networks**, the payment processors collaborate with the merchants' acquiring banks and do not have a direct contractual relationship with merchants (e.g. Visa and Mastercard). This means that these credit card companies 'rely on a third-party acquiring or issuing bank to take action against a merchant should the bank suspect wrongful activity by the merchant' ([12]).

- **Debit cards**: cover payments that imply an 'immediate' or 'near-instant' deduction of the funds for the individual transaction from the cardholder's account. 'This can make it difficult for consumers to handle a dispute/chargeback, since there is typically no extra protection of the funds in a debit account' ([13]).

- **Direct payment** (or payment initiation services) ([14]): allows users to make a one-off payment or set a direct debit from their bank account, online or through a mobile application (app). As regards payers, online or mobile applications of most banks provide this kind of service. As regards payees, a number of services allow them to accept direct payments in Europe, such as Bancontact, GiroPay, iDEAL or Przelewy24.

- **Money transfer services**: '[m]oney transfer operators (MTOs) are financial companies (but usually not banks) engaged in cross-border transfer of funds using either their internal system or access to another cross-border banking network' ([15]). In addition to traditional money transfer operators, a number of new digital services are being developed for quickly sending money across borders. This includes services such as Western Union or Transferwire.

- **Peer-to-peer (P2P) payment**: encompasses services or apps that are linked to a bank account or card and allow users to send one another money from mobile devices. Money received can

([12]) Office of the US IP Enforcement coordinator, 'Supporting Innovation Creativity and enterprise' p. 62.

([13]) OECD, WPIE paper on 'Online Payment Systems for E-commerce', 2006. See p. 19.

([14]) See European Commission 'Revised rules for payment services in the EU' that defines payment initiation services as services to initiate an order at the request of the payment service user with respect to a payment account held at another payment service provider.

([15]) IMF - 'International transactions in remittances' – 2009, p. 9.

be kept in the P2P payment service account or transferred to the associated bank account. This includes services such as Venmo, PingIt or Zelle.

- **Prepaid cards, electronic or mobile money**: provide new payment options, with national currencies stored as credits on a smart card or a system-provider's books ([16]). These prepaid cards are a 'category of payment instrument on which electronic money … is stored' ([17]). A cardholder can only spend the money loaded on the prepaid card ([18]). While '[g]eneral purpose prepaid cards have legitimate uses and constitute an instrument contributing to social and financial inclusion … anonymous prepaid cards are easy to use in financing terrorist attacks and logistics' ([19]). They are also used in the context of a number of IP-infringing activities.

- **Voucher systems**: consist in (re)selling vouchers for a number of digital services, and in particular cyberlockers ([20]) that can be used for copyright infringing activities. The voucher system act as an intermediary between the payment service provider (e.g. credit card) and the digital service. As a result, it can be used to circumvent measures put in place by payment services provider that are intended to counteract illegal activities ([21]).

2.1.2 Mediating services supporting the use of different electronic payment services

With the multiplication of electronic payment services, a number of services are being developed to facilitate their use by payers and merchants.

- **As regards payers**, digital or mobile wallets allow their users to pay with any payment method saved to their online and/or mobile account. This includes services such as Paypal, Apple Pay, Google Pay, PayU or WeChat Pay. Some of these services allow P2P payments or let their

([16]) Bank of England Quarterly Bulletin 2014 Q3 'Innovations in payment technologies and the emergence of digital currencies' p. 265.

([17]) See Regulation (EU) 2015/751 on interchange fees for card-based transactions, Article 2(35).

([18]) In the EU, anonymous cards must adhere to strict prescribed limits. See Section 3 on 'Regulatory requirements applying to different payment services'.

([19]) See Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Recital 14.

([20]) 'A cyberlocker is a type of cloud storage and cloud sharing service that enables users to upload, store and share content in centralised online servers.' See European Commission – Counterfeit and Piracy Watch List, SWD(2020) 360 final, p. 14.

([21]) Some cyberlockers services offer subscriptions through the resellers of these vouchers.

users move money from their bank accounts to their digital or mobile wallet and even provide different financial services. This is notably the case of Alipay ([22]).

- **As regards merchants**, mediating services can help businesses to move their payment processing online and accept a broad range of payment methods in a secure and user-friendly way. This includes services such as Stripe, Ayden or WePay.

2.1.3 Digital currencies

In addition to services and intermediaries supporting payments in currencies issued by central banks or governments, a growing number of digital currencies that can be used for electronic payments are also being developed.

- **Digital currency scheme**:

> incorporates both a new decentralised payment system and a new currency. … A key defining feature of each digital currency scheme is the process by which its users come to agree on changes to its ledger (that is, on which transactions to accept as valid). Most digital currencies are 'cryptocurrencies', in that they seek consensus through means of techniques from the field of cryptography ([23]).

This includes Bitcoin and Ethereum, as well as currencies providing an increased level of anonymity to make transactions untraceable, such as Dash or Monero. Some major technology companies have announced plans to develop cryptocurrencies, notably the Diem project ([24]). There are also a small number of digital currencies, such as Ripple, that seek consensus through non-cryptographic means.

- **Digital currency exchanges** are businesses that allow customers to trade cryptocurrencies or digital currencies for other assets, such as conventional currencies, or other digital

([22]) Butterwroth Journal of International Bankin and Financial Law – 'Decoding Alipay: Mobile Payments, a cashless society and regulatory challenges' – January 2018.
([23]) See 'Innovations in payment technologies and the emergence of digital currencies', Bank of England Quarterly Bulletin 2014 Q3, p. 265.
([24]) See White Paper from the Diem Association Members.

currencies. They are key intermediaries as they act as the entry and/or exit points for IP-infringers using digital currencies. Well-known digital currency exchanges include CoinBase, Kraken, CEX.IO or Coinmama.

2.2 Scope of the analysis

The identified payment services are all misused to different extents in the context of IP-infringing activities. There are no studies focusing specifically on the misuse of payment services to support IP-infringing activities, but a series of EUIPO Observatory reports on 'Online business models infringing IPRs' provides indications on the most common payment mechanisms used to support different business models ([25]). The Intellectual Property Crime Threat Assessment 2019, carried out by the EUIPO in collaboration with Europol, also identifies some of the sources of revenues and payment mechanisms used for IP-infringing activities ([26]).

These reports provide an overview of the payment services commonly misused for IP-infringing activities, in particular, credit cards, prepaid cards, money transfer services, as well as mediating services. In the context of this discussion paper, experts agreed to focus the analysis on these services.

Digital currencies are also identified as a payment method in a number of online business models that infringe IPRs. These are likely to gain popularity for that purpose as their adoption rates with end users increases. However, this use is still relatively limited, and since digital currencies are creating a number of new challenges, experts agreed to keep them out of the scope of this analysis and consider a specific analysis at a later stage.

Likewise, advertisements (ads) appearing on IP-infringing websites are identified as a source of revenue for a number of online businesses that infringe IPRs. The payment for these ads could be considered a payment mechanism. As above, experts agreed to keep 'payment for ads' out of the scope of this analysis and consider a specific analysis at a later stage.

([25]) See EUIPO Observatory 'Research on online business models infringing IPRs – Phase 1', 2016 - 'Suspected trade mark infringing e-shops utilising previously used domain names: Research on online business models infringing IPRs – Phase 2', 2017 - 'Illegal IPTV in the European Union: Research on online business models infringing IPRs – Phase 3', 2019.

([26]) See EUIPO and Europol joint study 'Intellectual Property Crime Threat Assessment 2019'.

3 Regulatory requirements applying to payment services

Payment services deal with a very large number of transactions and their services can be misused for all kinds of illegal purposes. Unlike other types of intermediaries, they are subject to strict regulatory requirements regarding fraud and illegal activities. These requirements provide several ways for payment services to identify suspect users and the use of their services, and to counteract this use. This has led to the development of a number of good practices that counteract illegal activities, including IP-infringing activities.

Credit, e-Money and payment institutions, as well as crypto-asset exchange providers, are notably subject to anti-money laundering (AML) regulations. The level of obligation they are subject to may vary depending on the type of provider and the type of services provided. In the EU, applicable legislations are based on international standards set by the Financial Action Task Force (FATF)([27]) (which includes different EU Members States and the European Commission as members), and the successive EU Anti-Money Laundering Directives([28]).

The EU adopted the first AML Directive in 1990, imposing on 'obliged entities' to apply **customer due diligence requirements**, namely identify and verify the identity of clients including beneficial owners, **monitor transactions** and **report suspicious transactions** to relevant authorities. This Directive has been regularly revised to mitigate risks related to money laundering and terrorist financing, and the EU has considerably strengthened its legal framework in recent years.

Obliged entities([29]) covered by AML regulations must meet certain day-to-day responsibilities. As indicated, these include carrying out 'customer due diligence' to check that their customers are

([27]) The FATF 'is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. [Its] objectives … are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.'

([28]) See European Commission on 'Anti-money laundering and countering the financing of terrorism'.

([29]) These entities are defined in Article 2 of Directive (EU)2015/849 (4th AML Directive), and notably include credit and financial institutions. The 5th AML Directive (Directive (EU) 2018/849) further extends the scope of entities covered and notably the one dealing with cryptocurrencies, adding 'providers engaged in exchange services between virtual currencies and fiat currencies' and 'custodian wallet providers'.

effectively who they say they are, and assessing the risks connected with their businesses. There are three levels of customer due diligence.

- **Simplified due diligence**: only requires the obliged entity to identify the customer. There is no requirement to verify the customer's identity. This is the lowest level of due diligence that applies when there is little opportunity or risk for the obliged entity services or customer becoming involved in money laundering or terrorist financing.

- **Standard due diligence**: requires the obliged entity to identify their customer as well as verify their identity. It also includes a requirement for obliged entities to gather information to enable them to understand the nature of the business relationship between the payer and payee. This is the level of due diligence required in most cases in situations where there is a potential risk of money laundering, but it is unlikely to realize.

- **Enhanced due diligence**: entails a series of due diligence activities that are dependent on the nature and severity of the risk. The additional due diligence can take many forms, from gathering additional information to verifying the customer's identity or source of income or even running an adverse media check([30]). This level of due diligence is required when a customer and product/service combination poses a greater risk of money laundering so as to mitigate this increased risk.

In addition, specific methods of identity verification are defined at Member State level.

Obliged entities must also put in place **internal controls and monitoring systems**. The nature of these controls is on a risk-based approach and will depend on the size and complexity of their activities, including the number of customers they have and the number and type of products and services they provide.

Finally, obliged entities have to **report any suspicious activity** to the national Financial Intelligence Unit (FIU). The core function of an FIU is the receipt, analysis and transmitting of reports of suspicions identified and filed by the private sector. The FIUs therefore function as

([30]) The 5th AML increases the focus on digital customer due diligence and encourages the use of automated adverse media screening.

an intermediary between the private entities, subject to [reporting] obligations, and law enforcement agencies. … A key element in the functioning of FIUs is their ability to cooperate both with foreign counterparts, as well as with other national institutions ([31]).

The 5th AML Directive that had to be transposed by Member States by January 2020 introduced substantial improvements that notably limit the anonymity related to virtual currencies, wallet providers and pre-paid cards. Under this Directive, Member States are only authorised to allow the anonymous use of electronic money products: (i) when customers use their prepaid instrument (such as prepaid cards) directly in the shop for a maximum transaction amount of EUR 150; or (ii) when customers carry out an online transaction with a prepaid card below EUR 50.

Experts noted that the sale of counterfeit goods was considered a suspicious activity and should be monitored and reported by obliged entities. The 6th AML Directive that had to be transposed by Member States by December 2020 harmonised the definition of money laundering across all Member States ([32]). It defined 22 offences for money laundering, including the 'counterfeiting and piracy of products', and made aiding and abetting money laundering a criminal act ([33]).

New legislative package on countering money laundering and financing of terrorism

Experts noted that AML regulations were continuosly evolving, pointing to the package of legislative proposals presented by the European Commission in July 2021 aimed at strengthening the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules ([34]). It includes the following four legislative proposals:

- a new regulation on AML / Combating the Financing of Terrorism (CFT), which will contain directly applicable rules, including in the area of customer due diligence and of beneficial ownership;
- a 6th Directive on AML/CFT, which will replace the existing Directive 2015/849/EU, containing provisions that will be transposed into national law, such as rules on national supervisors and financial intelligence units in Member States;
- a revised regulation on the transfer of funds that will make it possible to trace transfers of crypto-assets;
- the creation of a new EU authority to fight money laundering.

([31]) See Council of Europe website on Financial Intelligence Units,.

([32]) Directive (EU) 2018/1673 on combating money laundering by criminal law, 23 October 2018.

([34]) See European Commission 'Anti-money laundering and countering the financing of terrorism legislative package', 20 July 2021.

The different levels of due diligence and related obligations of payment services to on-board and/or monitor the activities of merchants depending on their activities are reflected in a number of good practices by payment services that are seeking ways to limit the risks of their services being misused for IP-infringing activities (Section 5).

4 Emerging trends and challenges

Electronic payment services providers, IP owners and law enforcement authorities are facing a number of challenges in counteracting the misuse of payment services for IP-infringing activities.

4.1 Transaction laundering and the new challenges to address it

The development of electronic payment services and e-commerce is offering unprecedented opportunities for businesses to quickly set up and develop their activities. However, this dynamic and fast changing environment also offers new opportunities for sophisticated money-laundering schemes, including for the counterfeiting and piracy of products.

It has notably given rise to 'transaction laundering', also known as 'unauthorised aggregation' ([35]). In the card payment system, this involves the processing of the card sales of one merchant through the merchant account of another. As regards e-commerce sales, it generally consists of channelling payments for illegal transactions through a website that is or looks perfectly legitimate, with or without the knowledge of the merchant that is responsible for that website and the associated card account. The laundered transactions may be illegal and/or violate the payment service terms of use. For example, the transactions for a website selling counterfeit products can be channelled through a website that appears to sell perfectly legitimate products. It is estimated that 'about 50 %–70 % of

([34]) See European Commission 'Anti-money laundering and countering the financing of terrorism legislative package', 20 July 2021.

([35]) There are different forms of transaction aggregations, including 'Compliant Aggregation' (through a payment facilitator for example), 'Non-Compliant Aggregation' (that happens by mistake, when a merchant sells the same products via another website) and 'Illegal aggregation' (that is intentional transaction laundering covered by this section).

online sales for illicit drugs, counterfeit goods, and unlawful content involve some form of transaction laundering' ([36]).

Transaction laundering can be difficult to detect ([37]) and is addressed through sophisticated monitoring of transactions and websites to detect illegal activities, and in particular websites that are not reported to the acquirer by the merchant but where the illegal activities are actually taking place. This can involve tracking addresses, billing descriptors and contact details throughout the web, as well as scanning the entire internet protocol range of the reported website looking for similar pages (Section 5.1.2).

The development of innovative payment services is in some instances challenging existing monitoring techniques. In this context, experts pointed out the development of P2P payments (Section 2.1.1) and the challenges they raise with regard to detecting transaction laundering. According to the experts, although some P2P payment providers had sophisticated monitoring systems in place to flag activities that were not personal but commercial in nature, this was not the case of all providers.

4.2 Identifying IP infringers across different payment and intermediary services

The misuse of e-commerce marketplaces services to facilitate the sale of counterfeited or pirated products also raises new challenges for payment service providers. IP infringers selling their products through e-commerce marketplaces do not need to set up a website and register as a merchant with a payment service. They can simply set up an account with the e-commerce marketplaces, and have buyers use all the payment options supported by the marketplace (e.g. credit or debit cards, direct payment, electronic or mobile money).

Some of the major e-commerce marketplaces have their own electronic payment services and are registered as payment and e-money institutions. As part of these activities, these institutions can engage in fraud detection and prevention of risks. Many e-commerce marketplaces also have notice-and-action mechanisms, allowing IP owners to notify listings potentially infringing their rights. A few

([36]) The Growing threat of transaction laundering, Thomson Reuters.

([37]) White paper on: Transaction laundering – A growing threat in the payment industry, Infosys, 2018, p. 3.

e-commerce marketplaces also have 'IP protection programmes' ([38]) to support the cooperation with IP owners and put in place preventive measures. These different measures support the detection of IP-infringing listings and, in some instances, the termination of IP infringers' accounts.

Virtual bank accounts ([39]) are sometimes used by sellers on e-commerce marketplaces when trading internationally ([40]). They can also be used by IP-infringing sellers to obfuscate their identities and the final destination of the payment, and to rapidly set up a new seller account when their accounts have been terminated.

In this context, some e-commerce marketplaces are also putting in place measures to better identify the bank accounts of sellers, where they direct payments and the actual person receiving those payments. This includes measures to verify the seller and related bank account information, as well as measures to limit payments to certain bank accounts. Amazon, for example, has developed its 'Payment Service Provider programme' so as to limit payments to virtual bank accounts from payment services meeting certain requirements for 'risk and compliance controls [, as well as] exchange information with Amazon to reduce the potential for fraud and to make it even harder for bad actors to hide.' ([41])

Some experts noted that credit card networks have developed databases of terminated merchants (or Terminated Merchant Files, See Section 5.1.3) that list merchants and related accounts that have been closed by credit card processors for a high number of chargebacks or laundering, among other violations of the credit card terms and conditions. These databases can be used to limit the use of credit card payments by repeat infringers.

In this context, they highlighted the opportunity to extend information-sharing with e-commerce marketplaces so that they can identify potentially problematic merchants that have been terminated

([38]) A few examples include Alibaba 'IP protection platform', Amazon 'Brand Registry', or Ebay 'Verified Right Owners' programme (VeRO), or Allegro 'Rights Protection Cooperation Program'. The EUIPO Observatory web page on 'Protecting your IP rights on e-commerce marketplaces' provides further information on the IP protection mechanisms of a number of e-commerce marketplaces.

([39]) Traditional bank accounts typically require the account holder to open up the account in person in a bank office, and provide a number of documents including registration in the relevant country. With virtual bank accounts the process to open up the account and operate it take place entirely online, and may not require registration or presence in the relevant country.

([40]) Virtual accounts can notably allow sellers trading internationally to receive payments in their buyers' local currency.

([41]) See Amazon Brand Protection Report, May 2021, p. 6.

by credit card networks, and provide information about terminated sellers that may try and gain access to credit card network services. Experts explained that this would support the detection of repeat IP infringers trying to gain access to new e-commerce marketplaces and/or payment services when their accounts are terminated. They also acknowledged the legal and technical complexity of putting such systems into place.

4.3 Sharing of information

The experts identified an overarching challenge of sharing of information between electronic payment service providers and law enforcement authorities, as well as between private players. This sharing of information is considered a key element in enabling payment service providers to prevent the misuse of their services for all sorts of illegal activities, including IP infringement. In this respect, two different types of information can be distinguished.

- **Information about IP-infringing products and services**: this non-personal information supports the detection of illegal activities using payment services. Experts noted that it is central for payment service providers to gain access to information from IP owners to effectively identify IP-infringing products and services. With the exception of products that are blatantly sold as counterfeits, payment services providers generally need the IP owner's confirmation that a product is effectively infringing their IP rights before taking action. The sharing of such non-personal information by IP owners([42]) can contribute to the proactive identification of counterfeit items.

  As regards IP-infringing services and, in particular, piracy websites, some experts highlighted the importance for the risk assessment and monitoring of some website activities to take into consideration existing illegal websites lists. In Denmark, for example, a list of websites that have been ruled illegal is made available to advertising and payment service providers that voluntarily commit to block payments to these sites (Section 5.2.2).

- **Information about IP infringers**: this information supports the detection of individuals or legal entities that may use different payment services from different countries and/or move from one

([42]) e.g. guidance on the fact that the first sales of a new product is limited to its official website.

payment service to the other when the illegal nature of their activities is detected. Experts noted the challenge with regard to payment services sharing personally identifiable information with various players.

- **Law enforcement authorities**: if obliged entities have to report suspicious activities or transactions (Section 3), experts noted the limits to submit multi-country reporting to national authorities. They highlighted the importance of such multi-country reporting to effectively support relevant law enforcement investigations in the context of complex illegal activities occurring across many countries.

- **Between private players**: experts stressed the need for guidance that would detail what information could be shared in line with EU data protection and competition laws. With regard to data protection, they pointed to the European Commission IP Action plan and the announced 'EU Toolbox against counterfeiting', which highlight that a fundamental element in the fight against counterfeiting 'is the sharing of relevant data on products and traders in compliance with EU data protection law, for which further guidance may be necessary' ([43]).

A number of good practices exist or are being developed to address some of the challenges raised by the misuse of payment services for IP-infringing activities.

5 Good practices

Payment service providers are in a unique position to identify IP infringers and stop payments related to IP-infringing activities. They have developed a number of policies, procedures and initiatives in that field. This section explores a number of good practices that have been identified by experts.

([43]) Commission Communication Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience, COM(2020) 760, November 2020, p. 16.

5.1 Preventive measures

A number of good practices are in place to pre-empt the misuse of payment services.

5.1.1 Terms and conditions

Depending on the payment services and intermediaries, different terms and conditions may apply to merchants, entities acquiring merchants, and payers. Experts have identified a number of good practices in these different terms and conditions or policies that specifically address transactions related to IP-infringing activities ([44]).

- **Terms and conditions applying to merchants, or entities acquiring merchants**. These include the following.

    - **Prohibition of activities infringing or facilitating the infringement of IP rights**: this is for example the case of Stripe that prohibits the use of payment services for a **number of business activities and practices** considered as 'Restricted Businesses' ([45]), including businesses selling 'any product or service that directly infringes or facilitates infringement' of IPRs.

    - **Specific obligations for acquiring entities, with regard to certain activities**: For example, Mastercard and Visa require enhanced due diligence reviews and/or monitoring obligations on acquiring entities with regard to certain activities. Mastercard's 'Security Rules and Procedures', for example, provide a detailed set of criteria for it to decide if a cyberlocker should be considered as a high-risk merchant, including whether the cyberlockers provide 'rewards, cash payments, or other incentives to uploaders [including] a higher commission for the distribution of file sizes consistent with long-form copyrighted content such as movies and television shows.' ([46]). Another example is 'Visa Merchant Risk Monitoring', which requires the acquirer to '… have measures in place to

([44]) Below are just a few examples as the desk research based on the experts' inputs only focused on a limited number of payment service providers.

([45]) See Stripe's web page on Restricted Businesses.

([46]) See Mastercard Security Rules and Procedures – Merchant Edition, 9 February 2021, Section 9.4.6, p. 82.

periodically review websites of ecommerce merchants on a risk-prioritised basis', and notably '… a scan for products or services violating Visa rules or laws in the seller's and/or buyer's jurisdiction.' ([47])

- **Suspension of the payment as well as the payee's guarantees or protection**: For example, PayPal has a user agreement listing 'Restricted Activities' and forbidding the use of its services to infringe IP belonging to third parties and a specific prohibition to sell counterfeits ([48]). Engaging in these activities may lead not only to the termination of the user agreement, but also to the suspension of the PayPal Seller Protection Program ([49]). PayPal may also contact buyers who have purchased goods or services from the relevant seller, the seller's bank or credit-card issuer, as well as 'other impacted third parties or law enforcement'. PayPal can also hold funds temporarily if the payment sent to the seller 'is challenged as a payment that should be invalidated and reversed' ([50]).

- **Terms and conditions applying to payers – chargeback process for counterfeits**: For example, Mastercard provides its clients with a chargeback process in case the goods purchased using its services are counterfeited. The process consists in a request for transaction reversal to secure a refund for the purchase. The cardholder has to:
  - fill a dispute resolution form – cardholder dispute chargeback ([51]);
  - as well as indicate the disposition of the good (i.e. possession of customs, cardholder, etc.);
  - provide proof that the good is counterfeited,
  - as well as fulfil additional formal requirements ([52]).

Some experts suggested that terms and conditions providing a clear prohibition of the use of their services for IP-infringing activities, with a broad definition of these activities, constituted good practice. Similar to the terms and conditions of a number of online intermediaries (e.g. e-commerce

([47]) See Visa Global Acquirer Risk Standards, 1 October 2018, Section 7.5, p 31.
([48]) See PayPal's restricted activities.
([49]) See PayPal's seller protection program.
([50]) See PayPal's 'Actions we may take'.
([51]) See Mastercard chargeback guide, p. 48.
([52]) Ibid., p. 396.

marketplaces), they suggested that terms and conditions could also set clear repeat infringer policy, leading to the termination of the accounts of repeat infringers.

5.1.2 Third-party certification services

Specific obligations for acquiring entities are also applied by some payment services to online pharmacies. Both Visa and Mastercard, for example, require acquiring entities for this type of merchants to verify that their activities effectively comply with all applicable laws, including through accreditation with a recognised third party ([53]). In this context, experts pointed to the '.Pharmacy Verified Websites Program' of the National Association of Boards of Pharmacy (NABP) and its recognition as a third-party certification service by Visa and Mastercard as a good practice.

As part of the process to register a '.pharmacy' domain name (that is only available to pharmacies and other entities offering prescription drugs and related information and services), the NABP verifies that an online pharmacy complies with all applicable regulatory requirements. Once verified, NABP approves the registration of the '.pharmacy' domain name, and adds it to its list of verified websites ([54]).

Experts also pointed to the European Medicines Agency (EMA) website, which lists the EU Member States registers of online medicine retailers and can be used to verify that an online pharmacy is effectively registered with the relevant national competent authorities ([55]).

Experts highlighted that these good practices counteracted the misuse of payment services by illegal online pharmacies, including pharmacies selling counterfeit medicines.

5.1.3 Systems to identify high risk merchants

A number of credit card networks, including Mastercard, Visa or American Express, have developed databases of terminated merchants known as 'Terminated Merchant Files' (TMF). These TMF list

([53]) See for example: Visa – Online Pharmacy Guide for Acquirer, June 2016, p. 33.
([54]) See NABP web page on Digital Pharmacy.
([55]) See EMA web page on Buying medicines online.

merchants and related accounts that have been closed by different credit card processors for high chargebacks (i.e. credit card users' requests for a transaction reversal to secure a refund) or violation of the credit card terms and conditions (e.g. sale of product and services infringing or facilitating the infringement of IP)([56]). 'All [credit card] processors must check a TMF when accepting a new user and are also required to add merchants to a TMF if the account is closed and meets TMF criteria'([57]).

For example, Mastercard has developed the 'Mastercard Alert to Control High-risk Merchants' (MATCH). It 'allows an acquiring partner to lookup whether another acquiring partner has terminated a merchant in the past and the reason for that termination, to aid in an onboarding decision'([58]). Acquiring partners terminating a merchant have 5 days to submit information on the merchant and the applicable reason code for the termination.

It is interesting to note that the MATCH system not only finds an exact possible match when a data lookup function matches the record of a terminated merchant, but also possible phonetic matches, as the system 'converts certain alphabetic data, such as Merchant Name and Principal Owner First and Last Name to a phonetic code. The phonetic code generates matches on words that sounds alike … The phonetic matching feature of the system also matches names that are not necessarily a phonetic match but might differ because of a typographical error … or a spelling variation…'([59]).

TMF and systems like MATCH that, inter alia, cover merchants that have been terminated for IP-infringing activities, allow acquirers to access risk information before entering into a merchant agreement, resulting in many instances in the acquirer refusing to make an agreement with a terminated merchant. In that respect, they constitute a good practice in limiting the use of credit cards payment by repeat IP infringers.

([56]) These TMF have not been set to target specifically merchants infringing IP, but to cover a broad range of terms and conditions violations, and high chargebacks that can occur for a broad variety of reasons (e.g. bad client service).

([57]) See Stripe web page on 'High risk merchant lists'.

([58]) See Mastercard developer web page on 'MATCH'.

([59]) See Mastercard developer web page on 'MATCH Documentation'.

5.1.4 Systems to monitor merchants

The regulatory framework applying to regulated entities establishes a risk-based approach, with transaction and client status monitoring, and risk assessment (Section 3). The actual risk assessment is largely left to regulated entities. In this context, credit card systems such as Mastercard have established the Merchant Monitoring Program to encourage acquirers to use Merchant Monitoring Service Providers (MMSPs). These are vendors hired by an acquirer to conduct merchant website URL content monitoring and to identify potential transaction laundering (Section 4.1).

The use of an MMSP allows acquirers to closely monitor the content of all or some of the merchants in their portfolio to ensure that no illegal or restricted goods are being offered for sale. MMSPs use a range of techniques for that purpose, such as internet traffic analysis to identify websites that have few to no visitors but report a large number of transactions, or the detection of links from the merchant's disclosed website to other undisclosed websites that may be offering illegal items for sale. Some experts noted that the activities of some MMSPs were not limited to payment and can be used by other types of intermediaries – in particular advertising intermediaries – in the context of their activities ([60]). Experts also underlined that some payment service providers had developed their own merchant-monitoring systems and did not rely on the services of MMSPs.

5.2 Reactive measures

A number of the identified good practices are in place to address the actual misuses of payment services in the context of IP-infringing activities.

([60]) See Verisk's G2 Business Announces New Strategic Alliance with National Associations of Boards of Pharmacy (NABP), with certification by NABP of healthcare merchants, allowing these merchants to fulfil Visa and Mastercard requirements for card-not-present transactions, but also advertising criteria from Google, Bing, Yahoo!, Twitter and Snapchat.

5.2.1 Notification systems

Some payment service providers have put in place mechanisms for IP owners to notify them of suspected IP-infringing activities using their services and that can lead to them taking action directly, or to request action from the suspected merchant's acquirer.

- **Notification with action from the payment service itself**: For example, both Stripe ([61]) and PayPal ([62]) provide online forms for IP owners to report suspected IP-infringing activities. As part of the notification system, IP owners or their authorised representative are typically asked to provide:

  - information on the infringed IP rights (e.g. a trade mark registration number);
  - the URL leading to the specific goods or services infringing their rights;
  - details on how these specific goods or services are infringing their rights.

  Upon notification the payment service provider reviews the IP owners' claims, and can decide to take action, including the suspension or the termination of the use of the payment service.

- **Notification with action from the acquiring bank**: some of these notification mechanisms require the bank of the merchant suspected of IP-infringing activities to perform specific due diligence or take action. Visa, for example, has put in place a system to provide assistance to IP Owners to address e-commerce transactions involving IP-infringing products. Upon notification with evidence from an IP owner that a merchant is involved in the online sale of IP-infringing goods using Visa-branded payment cards, Visa attempts to identify the merchant and notifies the merchant's acquiring bank. Visa requests the bank to take 'appropriate action', including requiring the merchant to stop selling the IP-infringing goods identified by the IP owner. If the merchant does not demonstrate the authenticity of the goods and the lawfulness of the sale, the bank is expected to terminate processing 'Visa payments' for this merchant ([63]).

  Similarly, Mastercard has established a system for law enforcement authorities and IP owners to notify merchants selling IP-infringing products or services. Upon receipt of a full notification,

([61]) See Stripe's Restricted Business Intellectual Property ('IP') Notice Process.
([62]) See PayPal Infringement Report Policy.
([63]) See Visa - Intellectual Property.

Mastercard sends it to the relevant acquirer, asking it to investigate the alleged illegal activity and to provide a written report on the results of its investigation. If the acquirer determines that the merchant is engaged in IP-infringing activities, it has to terminate the merchant's account or ensure that it ceases accepting Mastercard payment for the incriminated product or services ([64]). If it terminates the merchant's account, the acquirer has to list it in Mastercard's terminated merchant MATCH system.

5.2.2 Collaboration with IP owners

- **Danish Codex**: in order to counteract the financing of online IP-infringing activities, and in line with the so-called 'follow-the-money' approach, the Danish Rights Alliance is collaborating with the Danish Ministry of Culture and ads and payment service providers that voluntarily commit to 'prevent ads, payment, and traffic from legitimate businesses from ending up on illegal services.' The Right Alliance has established 'a list of information about websites that have been ruled illegal by the courts' and makes it available to the Ministry of Culture, which forwards it to the signatories to the Codex agreement that 'blocks ads on and payments to convicted illegal services'. This list of illegal websites has been in use since February 2020 ([65]).

- **RogueBlock**: is a collaborative project between the International Anti-Counterfeiting Coalition (IACC) and major credit card and financial companies. ([66]) It aims to facilitate and accelerate action against counterfeiters' merchant accounts. It consists of a simplified procedure for rights holders' representatives to report online sellers of counterfeit 'directly to credit card and financial service companies'. Rights holders' representatives have access to the system through a dedicated online portal that facilitates the flow of information with law enforcement authorities, as well as credit card and financial services companies. The online portal allows them to submit a report on infringing websites or sellers on online marketplaces. The IACC reviews each report before passing it to the relevant credit card and financial services

([64]) It is interesting to note that '(if) the Merchant is located in a country where the online sale of the alleged Illegitimate Product does not violate applicable country laws, the Acquirer must suspend or terminate acquiring sales by that Merchant to account holders of accounts issued in countries where the sale of the alleged Illegitimate Product is illegal or is otherwise prohibited by local law.'

([65]) RettighedsAlliancen 'Annual Report 2020', p. 22

([66]) EUIPO - 'Study on voluntary collaboration practices in addressing online infringement of trade mark rights, design rights, copyrights and rights related to copyright', September 2018, p. 23.

company([67]). Rights holders' representatives can review the status and outcome of their reports through the same portal.

The programme has led to the termination of 'over 5,000 individual counterfeiters' merchant accounts, which has impacted over 200,000 websites' ([68]). However, some experts underlined that the use of this programme by SMEs was undermined by the participation fee ([69]). They suggested creating a similar collaboration mechanism in the European framework. Other experts suggested that implementing such a collaboration could consist in creating a free-to-access European reporting portal, which might be a useful tool for facilitating reporting from all IP owners and, in particular, SMEs.

- **Voluntary cooperation agreements** are in place between IP owners and payment service providers to terminate the accounts of cyberlockers and internet protocol television (IPTV), subject to the provision of sufficient proof. Some experts also suggested implementing collaborations allowing rights holders to 'red flag' suspicious accounts and identify counterfeiters across different jurisdictions. They also suggested that communicating information (i.e. bank details of the infringers) regarding red flags and sellers of counterfeits to other payment services should be considered a good practice, subject to the application of EU competition and data protection laws.

- **'Committee on online payment good practices to protect copyright'**: in France, since 2015, payment intermediaries and rights holders have agreed to regularly meet under the umbrella of the Ministry of Culture ([70]). These meetings offer a platform to share information, including on IP-infringing websites, and to explain the legal and technical limits on the actions that can be taken by payment service providers. Some experts suggested that an EU approach, rather than a multitude of country specific initiatives, may be more effective and adapted to deal with the cross-territorial nature of IP-infringing website activities.

([67]) See IACC RogueBlock® Partners to the initiative include many of the biggest credit card and financial services companies in the world such as: MasterCard, Visa International, Visa Europe PayPal, MoneyGram, American Express, Discover, PULSE, Diners Club and Western Union.

([68]) Ibid.

([69]) Cour de comptes, 'La lutte contre les contrefaçons. Une organisation et des outils pour mieux protéger les consommateurs et les droits de propriété industrielle', 2020, p. 83, (French only).

([70]) See 'Lancement d'un comité de suivi des bonnes pratiques dans les moyens de paiement en ligne pour le respect du droit d'auteur et des droits voisin', 10 September 2015 (French only).

5.2.3 Collaboration with law enforcement authorities

This collaboration can facilitate the refunding of consumers that have mistakenly bought counterfeits. Moreover, there are a number of opportunities for collaboration with the aim of supporting law enforcement operations, as well as the sharing of intelligence on IP-infringing products and services.

- **Project Chargeback**: the Chargeback against fakes in Canada is a collaboration between the Canadian Anti-Fraud Centre (CAFC)([71]), credit card companies and banks, who work together to reimburse victims of online fraudsters and then close counterfeit retailers' accounts([72]). The Chargeback scheme is based on the contractual mechanism that links banks to payment service providers and prohibits any transactions related to fraudulent activities.

  Under this scheme, a consumer can file a complaint with the CAFC, providing information including details on the goods (usually by submitting a photograph), website address, date and purchase amount. With the help of rights holders, the CAFC confirms that the goods are effectively counterfeit and provide a certificate to the consumers. With this certificate and proof that the goods have been destroyed, the consumer can claim reimbursement directly from their bank.

  Based on its contractual obligations, the consumer's bank is required to report the fraud and breach of contractual obligations by the seller's bank to the relevant payment service provider. The seller's bank has to reimburse the consumer's bank and can be fined by the payment service provider. According to the CAFC, more than 12 000 chargebacks were made in 2018, and 45 000 since the implementation of 'Chargeback' in January 2013([73]).

- **Europol operations**: some experts suggested that the participation in such initiatives and the collaboration with the operations of Europol on stand-alone websites and social media would

([71]) CAFC is the Canadian institution responsible for consumer fraud

([72]) See WIPO Advisory Committee on Enforcement, 11th Session, Geneva, 5 to 7 September 2016.

([73]) Cour de comptes, 'La lutte contre les contrefaçons. Une organisation et des outils pour mieux protéger les consommateurs et les droits de propriété industrielle', February 2020, p. 83 and 84 (French only).

be relevant in tackling IP infringement. As examples of effective operations, experts highlighted:

- **Operation In Our Sites** (IOS), which is a recurrent joint global operation that was launched in 2014 to target websites selling counterfeit goods ([74]);
- **Operation Aphrodite,** in 2018 ([75]), 2019 ([76]) and 2020 ([77]) led to the seizure of counterfeit goods, closure of social media accounts and websites dedicated to IP infringement, and arrest of suspects.

The collaboration of the International Federation of the Phonographic Industry with the City of London Police (Police Intellectual Property Crime Unit – PIPCU), which has a dedicated IP crime unit and works with a number of financial institutions was also highlighted ([78]).

Some experts also suggested looking into collaboration and public-private partnerships related to other types of illegal activities, since they contributed to counteracting IP-infringing use of payment services and/or constituted examples of collaboration that could be used or replicated to counteract this specific use, including the following.

- **Europol Financial Intelligence Public Private Partnership**: Europol has been entrusted by EU Member States to create a European Financial and Economic Crime Centre (EFECC). As part of its mission statement, the EFECC is to '… enhance Europol's operational support to EU Member States and EU bodies in financial and economic crime and promote the consistent use of financial investigations', as well as to '… forge alliances with public and private entities to trace, seize and confiscate criminal assets in the EU and beyond.' In this context, it works on developing 'successful strategic cooperation and capacity building with relevant private and public actors in the margins of the Europol Financial Intelligence Public Private Partnership (EFIPPP)'. ([79]) This partnership brings together experts from major financial institutions and

([74]) See Operation In Our Sites (IOS), Europol.

([75]) See Europol, 'Social Media Crime: 20 000 packages of counterfeit medicine, mobile phones, jewellery, sunglasses and watch seized', 3 May 2018.

([76]) See Europol, 'Counterfeit crackdown hits two organised criminal groups with more than 30 suspects arrested', 13 June 2019.

([77]) See Europol; 'No safe market for fakes: 21 countries target illegal goods in Europe-wide sting', 25 September 2020.

([78]) See ICC/BASCAP, Report on the Roles and Responsibilities of Intermediaries, 2015, p. 91.

([79]) See European Financial and Economic Crime Centre – EFECC, Europol.

competent authorities from a number of EU Member States and non-EU countries, involving FIUs, law enforcement authorities and the European Commission, to improve transnational cooperation. Participants in the EFIPPP exchange strategic information and sanitised case studies. With the launch of the EFECC in June 2020, resources, such as the EFIPPP, are more accessible to Member States and FIUs for cross-border financial investigations in all criminal areas, including IP crime.

- **Cyber Defence Alliance in the United Kingdom (UK)**: this is a group of British-based banks and law enforcement agencies working together to share intelligence and fight against hackers and fraudsters ([80]). The UKIPO and the City of London Police have been looking closely at a similar model that might assist in developing private sector intelligence in the field of IP.

- **Anti-money laundering initiatives**: some experts considered that such initiatives were relevant for IP crimes, or as examples of collaboration with payment service providers. In this context, experts mentioned the Egmont Group ([81]) that provides a platform for 167 FIUs around the world to exchange suspicious transaction reports and other information relevant to money laundering with the aim of securely sharing expertise and intelligence.

  Other experts pointed to the Joint Money-Laundering Intelligence Task Force in the UK ([82]) as one example of a public-private partnership initiative to support financial information sharing. Within the EU, there are nine national level partnerships already established or in their preparatory stages. The majority of these partnerships are between national FIUs, financial supervisory authorities and representatives of private financial institutions, working on developing a more collective response to money laundering ([83]). These partnerships contribute to enhancing the focus on specific identified threats so as to provide timely and qualitative reporting in response to active investigations or live incidents, or to support asset recovery and other disruption of criminal networks ([84]). Here again, some experts suggested exploring how

([80]) See Europol: 'The Cyber Defence Alliance and Europol step up cooperation in the fight against fraudsters', October 2018.
([81]) See Egmont Group website.
([82]) See UK government: 'Anti-money laundering task force unveiled', February 2015.
([83]) See Future of Financial Intelligence Sharing Survey Report: Five_years_of_growth_of_public-private_partnerships_to_fight_financial_crime_-_18_aug_2020.pdf (future-fis.com).
([84]) ibid, p. 8.

to better share intelligence on money laundering activities related to the ‘counterfeiting and piracy of products’.

6 Conclusion

Payment service providers are in a unique position to identify IP infringers and stop payments related to IP-infringing activities. Unlike other types of intermediaries, they are subject to strict regulatory requirements to deal with fraud and illegal activities, such as different levels of due diligence to onboard their customers and/or to monitor their activities that vary on a risk-based approach. These regulatory requirements are reflected in a number of good practices developed by some payment services providers that are seeking ways to limit the misuse of their services for IP-infringing activities. This discussion paper will hopefully contribute to a better understanding of these good practices and contribute to the discussions on the challenges and opportunities to extend or replicate some of them to counteract IP-infringing activities.

PAYMENT – DISCUSSION PAPER
Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities

ISBN