EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

PAYMENT – DISCUSSION PAPER

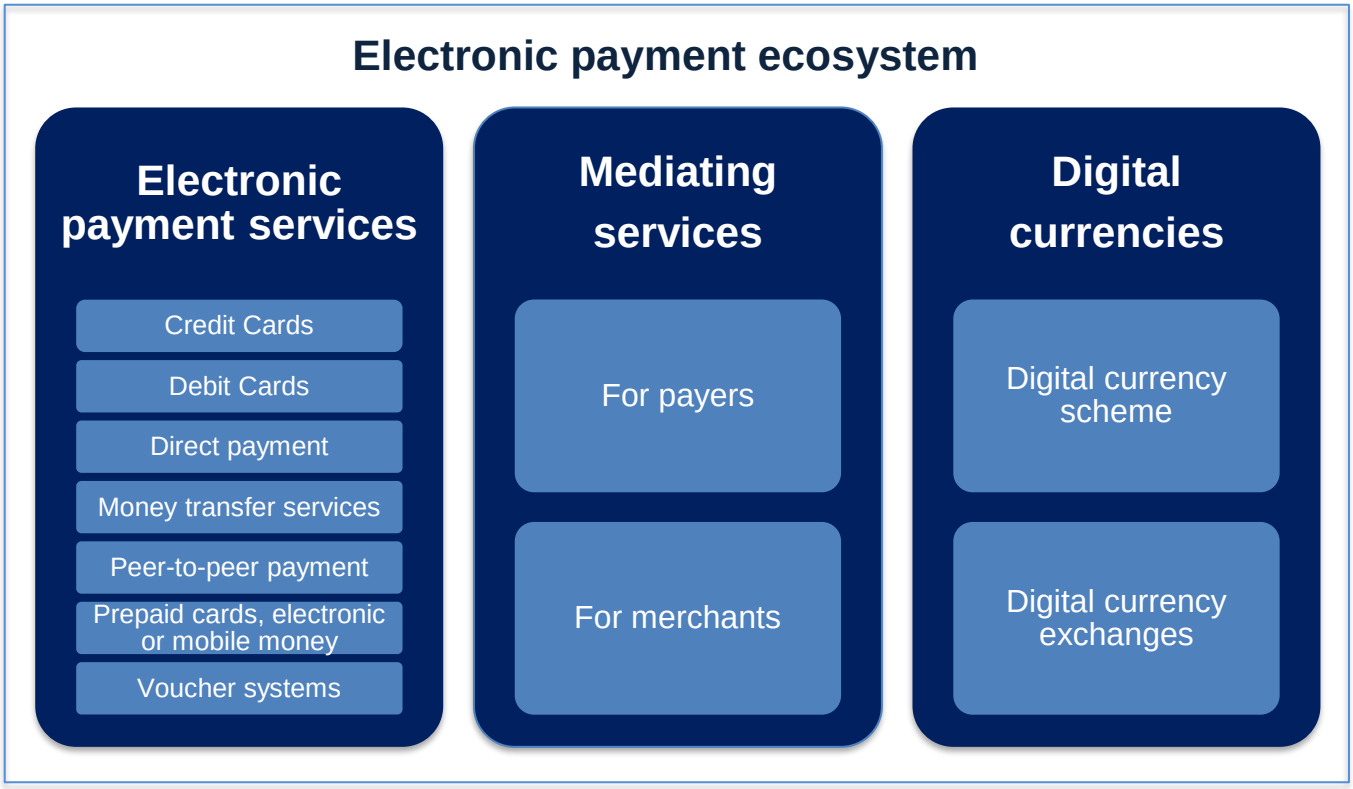
Challenges and good practices for electronic payment services to prevent the use of their services for intellectual property-infringing activities

Executive Summary

November 2021

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.

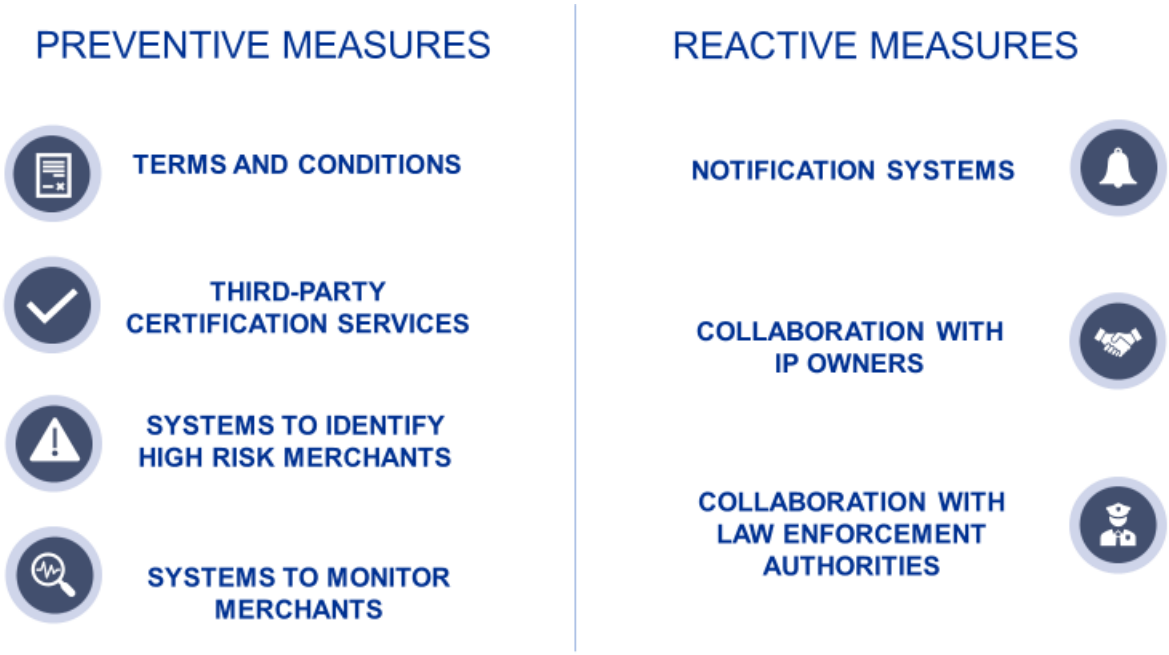
Unlike other types of intermediaries, payment service providers are subject to strict regulatory requirements to deal with fraud and illegal activities, and in particular money laundering. This includes:

- **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.

PAYMENT – DISCUSSION PAPER

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