AUDIOVISUAL ANTI-PIRACY ALLIANCE

JANUARY 2022

NEWS & VIEWS

SHOULD PAYMENT SERVICE PROVIDERS HAVE SELF-REGULATORY POLICIES IN PLACE TO HELP FIGHT AUDIOVISUAL PIRACY?

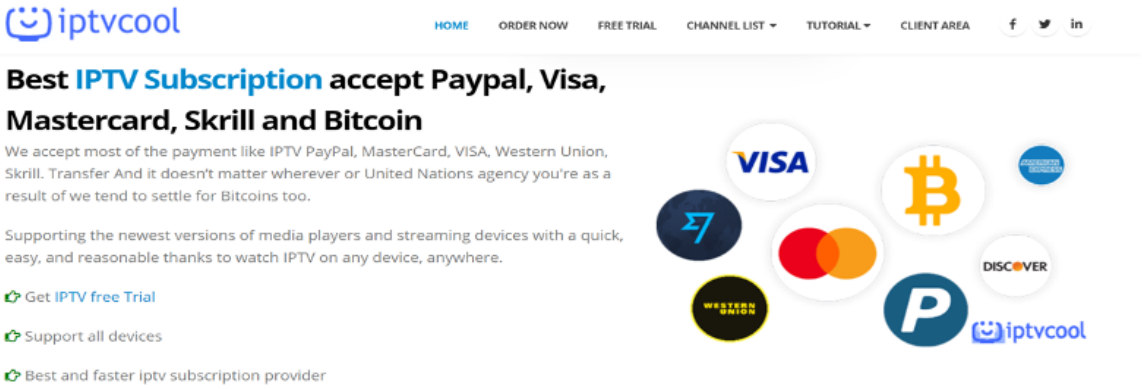
Recently the EUIPO Observatory on IP Infringements published a discussion paper on the Challenges and good practices for electronic payment services to prevent the use of their services for IP infringing activities. Based on input from one of its Expert Groups, the paper provides an overview on how such services are misused; what regulatory and other measures apply; emerging trends and challenges; and good practices adopted by payment providers which comprise both preventive and reactive measures. The discussion paper is a useful contribution to the debate about the role of intermediaries in facilitating – knowingly or not – IP crimes such as audiovisual piracy. However, closer scrutiny reveals that the practices in reality fall some way short of being "good".

Let's take a look at why and how online pirates exploit the trusted payment provider's brand. What procedures do

payment providers have in place to help to reduce piracy? And – crucially - what more can be done?

Using a household name to buy credibility

From a pirate's perspective, they want consumers to pay for the services they offer. Their professional- looking websites already fool many unsuspecting consumers into thinking that they are a legitimate vendor. This veneer of authenticity is further enhanced with pirates often using multiple well-known payment provider services to make it easier for subscriptions to be purchased. Pirate sites, such as the one below, with payment providers' logos have an air of legitimacy.



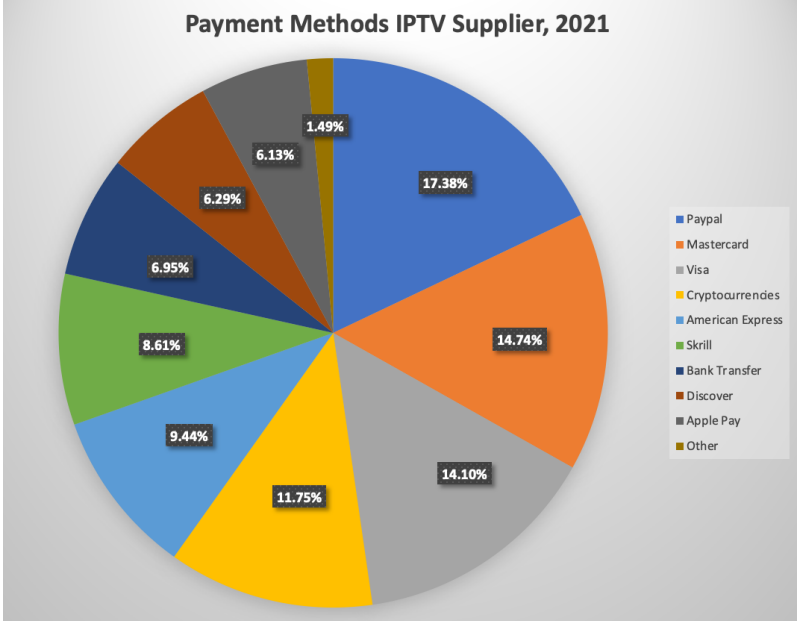
Example pirate site, displaying payment providers' logos

Positioning may vary, but the top 3 are the same

Just how prevalent is this practice of using familiar payment providers? It certainly isn't new. In 2018 Irdeto, a long-standing AAPA member, published some research which revealed that 76% of the sites surveyed advertised openly the payment methods available. Not surprisingly the familiar household names, Visa (21%), Mastercard (21%) and PayPal (14%) were used by the largest number of sites (56% in total).

Over the last few years, AAPA has engaged with all three companies and it is interesting to see what, if anything, has changed. Figures from a study carried out in 2021 by AAPA's Disruption Working Group show that the exploitation of the payment provider's trusted brand on pirate sites is a winning formula.

Yes, the results on page 3 are slightly different, but what is noticeable is that the top three facilitators for purchasing online pirate services are the same: albeit that they have switched positions and fallen in share (from 56% to 45%) as the use of cryptocurrencies has become more common. In AAPA's 2021 study, PayPal ranked first with 17%. Mastercard and Visa are jointly second with 14%.



AAPA 2021: Summary results

The question for the payment services industry and policymakers is how do so many sites slip through the net of the preventive measures – some of which are legal requirements like anti-money laundering regulations – described in the Observatory discussion paper. Of course, any ex-ante system is not watertight and can be circumvented but the evidence does suggest a lot more needs to be done. But by whom?

Varying levels of engagement

AAPA works with many parties to help fight piracy, providing awareness and training, operational support or finding *pragmatic* approaches to curb the impact of online piracy that can be accommodated by the different players. We do not expect third parties to exceed what they are able to do by law, by regulations applying to their own sector and limitations imposed by the organisational structure of the sector. As you'd expect, we're in discussions with the top three payment providers. What's the response so far?

Like all our interactions with different parties, there will always be those who are more able and willing to cooperate than others. The same is true with payment service providers.

PayPal and AAPA have a long-standing relationship. PayPal is committed to finding a workable solution to combat piracy's impact on the industry and on their brand. Issues are discussed openly and constructively.

From our interactions with Visa, we know that they have very stringent internal procedures in place. These procedures can include multiple cease and desist notices and may require proof via a test purchase. All of this takes time while piracy continues unchallenged. Visa is, of course, protecting its rights and interests, and AAPA members are doing the same. Maybe by working with parties together we can find a middle ground which reflects a balance of those interests in pursuing IP infringements.

As for Mastercard, it is a bit too early to say.

However, we are hopeful that engagement will be positive once it starts in earnest.

Being more proactive

From AAPA's perspective, there is much more payment service providers could do to help fight piracy. While the EUIPO Observatory Discussion Paper describes the various due diligence measures used by payment services, these need to be reinforced and monitored, preferably by a third party or via a MOU. A place to start would be to proactively monitor compliance with the payment service provider's terms and conditions.

The Discussion Paper also refers to procedures whereby payment service providers can enforce stay down measures. What are these? Once the payment service provider is satisfied that the complainant has provided enough evidence about an infringing pirate site, that payment service can terminate the contract with the user of the service. Unfortunately for stakeholders affected by piracy, this system is complex and too slow. It is also invisible to external parties, meaning that the industry has no knowledge of how specific repeat infringers are being treated or who has been classified as such. This may be the consequence of the sector's own regulatory regime but we should strive together for more transparency.

Know your business customer and stay down measures are facets on the Digital Services Act (DSA) which aims to combat the 'whack-a-mole' pirate site approach, whereby a pirate stream that has been removed will reappear within a matter of minutes. Does it make sense for payment providers to review and adopt working practices, such as those described in the DSA? AAPA certainly believes so.

Tackling cryptocurrencies

A curiosity of the EUIPO discussion paper is the omission of cryptocurrencies which are left to be discussed on another day. The use of cryptocurrencies is on the rise. In 2018 they accounted for only around 4% in the Irdeto analysis, but in 2021 they have now risen to almost 12% and this figure is likely to be higher in some countries.

The press would have you believe that the use of cryptocurrencies is exploding. Yes, as we have seen from our 2021 figures, there is some growth in the use of cryptocurrencies. Not huge, but there's an upward trend. You can surmise a few possible reasons as to why this uptake is not faster. These could be the instability of the cryptocurrencies, sinister association with hacking and ransom demands or that most consumers don't know how to use crypto.

Either way, the challenges posed by the growing use of cryptocurrency are well recognized by law enforcement agencies such as Europol and INTERPOL. Europol's recent Internet Organised Crime Threat Assessment 2021 describes how criminals obfuscate their illegal proceeds through the use of cryptocurrencies, privacy wallets and chain hopping amongst other methods. This

certainly makes the “follow the money” investigation route much harder. Yet, the growth trend does indicate there’s a need for law enforcement to stay up to date with the latest cryptocurrency techniques and AAPA is pleased to see Europol and INTERPOL strengthen their resources in this area.

Supporting more action

Yes, it’s always good to anticipate emerging problems, and the steady growth of cryptocurrency use is one such issue. However, we must not overlook traditional payment providers. They are still by far the most popular payment methods on pirate sites. More immediate action is needed to stem the volume of online piracy, and as key facilitators, payment service providers are well placed to play a positive role in this fight. Unfortunately, as we have seen over the years, it has proved challenging to introduce self-regulatory measures around these players.

The European Commission proposed in December 2013 that there should be a MOU for payment providers in the context of IP infringements. They sought to start discussions about how payment providers could assist in preventing the fulfilment of payments to IP infringers, but the MOU hasn’t seen the light of day. Given that the Commission has implemented two other MOUs – one for online platforms and counterfeiting and the second around advertising, it’s not because of a lack of experience on their side. Is it because the payment providers themselves don’t want to have self-regulatory policies in place? Or does the Commission need to be more aware of the harm which is being caused? Only they can answer that.

What’s incumbent on us, at AAPA, is to continue making consumers and policymakers aware of the payment service provider’s role in online piracy. The other is to educate, train, and advise all parties – including payment providers – in ways to tackle this growing threat. Finally, it requires all of us to act more responsibly and work together to stem the tide of digital content piracy. So, don’t wait for legislation to be in place – act now!

Sheila Cassells
Executive Vice President