

## **GREEN PAPER**

### **On on-line gambling in the Internal Market**

SEC(2011) 321 final

**Consultation Period:** until 31 July 2011

Introduction.

In general terms, we would like to highlight the following key issues for paysafecard in relation to online gambling:

- paysafecard has developed innovative payment solutions over the last ten years, assisted by funding from the Commission through the e-Ten project and promoted by EU legislation to promote the use of e-money. In particular, paysafecard is a market leader in prepaid cards for e-commerce, “(cash for the internet)”.
- These solutions are popular for on-line gambling, in particular as they enable players to participate with small amounts, without borrowing and using a payment method which needs to be procured from a “bricks and mortar” outlet and cannot be “topped-up” online. As such, paysafecard contributes to the fight against addiction. Moreover, paysafecard is regulated by the UK and Austrian financial services authorities (“passport” across the EU) and is fully compliant with AML legislation.
- While paysafecard is regulated as an e-money institution, paysafecard would be very concerned if it were to be made responsible for any aspect of online gambling regulation (such as customer verification), or if it were excluded from this market segment because of misconceptions concerning how paysafecard works. Such risks have already arisen in legislation proposed by some Member States.
- As expanded upon in the response to question 12 below, paysafecard requests that the Commission issue a Recommendation, confirming the place that e-money should have in the on-line gambling sector in the Internal Market and the positive role it can play.

#### **Questions relevant for paysafecard:**

#### **(10) What are the main advantages/difficulties associated with the coexistence in the EU of differing national systems of, and practices for, the licensing of on-line gambling services?**

As a payment services provider working cross - border in various EU Member States; this coexistence of different national systems regarding online-gambling services is a barrier to the business. As a payment operator it is not possible to control the acceptance and the usage of a payment solution depending on the countries and their individual licensing regimes.

The regulations regarding payment services for online gambling vary from state to state both when it comes to pay - in and pay - out. The payment operator must generally rely on the licensed operator to offer the payment solution in an compliant way.

#### **(12) Are there specific national regulations pertaining to payment systems for online gambling services? How do you assess them?**

Yes, there are various specific national regulations – some of them are still in a draft form.

## Examples:

**France:** There is a specific paragraph (Article 12) in the French online gambling regulations regarding payment systems for online gambling services. This paragraph imposes restrictions on the payout of winnings to only one payment account of the player.

Further there is a mechanism of financial institutions obliged to block funds of gaming websites operating in France without a licence.

Assessment: The French regulation ensures that all regulated European payment systems can participate in the French online gambling market. However, the restrictions regarding the payout of winnings and regarding the blocking of funds impose restrictions for payment services providers.

**Germany:** There is a specific paragraph (in § 4) in the German draft of the new online gambling regulation that sets a prohibition for payment services providers to provide services to gambling operators that operate illegal in Germany. This prohibition is not connected with an obligation of the German authorities to provide a “Black List” with the operators providing illegal online gambling services in Germany.

Assessment: In order to be compliant with this regulation payment services providers offering their services to German customers would need to do a constant monitoring whether any international gambling operators are targeting the German market without a licence. It would be the obligation of the payment services providers to assess what is an illegal online gambling service in Germany. In our view this assessment must be done by the German authorities and then communicated to the payment services providers!

**Greece:** There is a specific paragraph (Article 31) in the Greek draft of the new online gambling regulation that discriminates certain payment services providers with the following paragraphs: *Payment of the amounts for participation and profit payouts resulting from participating in gaming activities conducted via the internet must be conducted by financial institutions **having their headquarters or a branch in Greece.***

[...]

*Payment of monies for the participation in games of chance via the internet must be made to a licensed provider only, without any intermediation, except for financial institutions operating legally in this territory **in a manner that ensures the identification of the player**, as specifically defined in the Rules of Conduct and Monitoring of Gaming.*

Assessment: This draft clearly discriminates against financial institutions, which operate in Greece under the fundamental principle of the free movement of services by passporting their licence obtained in another Member State to Greece, without opening a branch. Moreover, it makes a link between the identification of the player and the financial institutions involved in the transaction of loading a player’s account. This obligation would make it impossible for a means of payment, which is based on the Simplified Due Diligence Rules set out in the 3<sup>rd</sup> Anti-Money-Laundering Directive, to operate in the market. If the identification of players were made an obligation of the financial institutions, then they could not possibly fulfil the obligation if they complied with the Simplified Due Diligence Rules under the Directive.

As can be seen from the above, several Member States have sought to interpret EU law restrictively. This has required the Commission to intervene on several separate occasions. It would surely be more efficient and less burdensome on business for the Commission to adopt a Recommendation setting out, clearly and unequivocally, the principles that the Commission was obliged to set out on an individual Member States basis, such as the attached correspondence.

**(14) What are the existing national rules and practices relating to customer verification, their application to on-line gambling services and their consistency with data protection rules? How do you assess them? Are there specific problems associated with customer verification in a cross-border context?**

In our view the customer identification should be undertaken by the operator and must be the operators' obligation. There should be no obligatory identification via the means of payment. This obligation would make it impossible for a means of payment, which is based on the Simplified Due Diligence Rules set out in the 3<sup>rd</sup> Anti-Money-Laundering Directive, to operate in the market. If the identification of players were made an obligation of the financial institutions, then they could not possibly fulfil the obligation if they complied with the Simplified Due Diligence Rules under the Directive. Many payment services providers would be excluded from the market of online gambling in case of an obligatory identification via the means of payment.

In addition, the payment landscape has recently started to change from bank driven products to more customer oriented solutions very often offered by non-banks. Most of these solutions do not have any identification obligation (Simplified Due Diligence) as they very often act in the space of micropayments ( up to 50 EUR e.g.). All these innovative solutions would be banned, even though they complied with EU law (Payment Services Directives, Anti-Money Laundering Directive, Second E-Money Directive).

**(24) Are on-line age controls imposed and how do these compare to off-line 'face-to face' identification?**

In our view the age verification should be undertaken by the operator and must be the operators' obligation. There should be no age verification system for online gambling via the means of payment. This obligation would make it impossible for a means of payment, which is based on the Simplified Due Diligence Rules set out in the 3<sup>rd</sup> Anti-Money-Laundering Directive, to operate in the market. If the age verification were made via the means of payment, then they could not possibly fulfil the obligation if they complied with the Simplified Due Diligence Rules under the Directive. Many payment services providers would be excluded from the market of online gambling in case of an age verification system for online gambling via the means of payment.

In addition, payment instruments can be intentionally or fraudulently transferred to third parties and therefore, they cannot act as a means of age verification.

Both licence regimes in Italy and France prove, the both customer identification and age verification should be conducted directly by the operator not via the payment solution, even though they complied with EU law (Payment Services Directives, Anti-Money Laundering Directive, Second E-Money Directive).

**(35) Do you have experience and/or evidence of best practice to detect and prevent money laundering?**

Paysafecard is subject to anti-money laundering and counter terrorist financing legislation in the EU. Applicable legislation includes:

- Member state implementation of the Third Money Laundering Directive 2005/60/EC
- EC Regulation 1781/2006 on information on the payer accompanying transfers of funds
- A number of counter terrorism and sanctions legislative provisions

Legislative provisions require issuers to address the risk of money laundering and terrorism financing that may arise from the use of their products by criminals. This entails a process of risk review, implementation of specific obligations set out in legislation and mitigation of risks that arise. The obligations are common to all financial services firms and comprise:

- Customer due diligence provisions; both initial and ongoing

Issuers are under a duty to verify the identity of customers where a business relationship has been established and to undertake ongoing due diligence processes to understand the nature of the business of the customer, on an ongoing basis. This is undertaken on a risk sensitive basis to ensure those areas that pose greater risk are given greater priority. This allows for simplified due diligence where the risk is low, full due diligence where the risk is increased, and enhanced due diligence where the risk is high.

- Reporting obligations

E-money issuers must have systems in place to be able to detect unusual transactions where these occur, and to then decide whether or not the transactions are also suspicious. Issuers' systems are calibrated for low value transactions and will seek to identify unusual patterns of purchasing cards or opening accounts, of loading funds unusual transactions and transaction patterns as well as requests for redemption. Where unusual activities are assessed to be suspicious, then a suspicious activity report will be made to the financial intelligence unit.

- Record keeping

E-money issuers are required under anti-money laundering legislation to keep records of transactions for 5 years from the date of a transaction, and to keep records relating to the identification of customers for the entire lifetime of the business relationship and for 5 years from its date of termination. This means that information is available to law enforcement investigators for a reasonable period, enabling the pursuit of suspected crime.

- Training of staff

Staff must be trained in both the legal obligations of regulated e-money issuers under anti-money laundering legislation and the practical means of recognising money laundering. This includes the internal escalation process as well as suspicious activity reporting to the relevant financial intelligence unit.

- Policies and procedures

Issuers are under a duty to put in place policies and processes that implement obligations relating to the various obligations, including: reporting of suspicious transactions, ML risk assessment and management, record keeping, and compliance monitoring.

**(50) Are any of the methods mentioned above, or any other technical means, applied at national level to limit access to on-line gambling services or to restrict payment services? Are you aware of any cross-border initiative(s) aimed at enforcing such methods? How do you assess their effectiveness in the field of online gambling?**

**See answer to question 12 above.**