I.B.L.J. 2011, 5, 555-568

International Business Law Journal

2011

# Securing the transfer of money in the new technologies context: the case of the French online gaming sector

Pauline **Le More**

Christelle Mazza



**Subject:** Banking and finance. **Other Related Subject:** Criminal law. Financial regulation. Hospitality and leisure

**Keywords:** Electronic funds transfer; Financial regulation; France; Money laundering; Remote gambling; Suspicious activity reports; Terrorist financing

## *555 INTRODUCTION

The emergence of the internet in the late 1990s, and the development of e-commerce in the early 2000s, led to the emergence of new economies. Legal impacts were felt in Europe both at Community and national levels. The decade that followed saw the development of innovative markets. As often then, the economy preceded the law and precedent regulation, despite the need for legal frameworks that shall protect the consumers and promote a safe financial system in general.

In the banking sector in particular, anonymous pre-paid instruments, such as gift certificates, restaurant vouchers, gift boxes or prepaid cards, have appeared recently. They have contributed to the upheaval of traditional banking. In order to provide for a legal framework, new regulation has emerged through Directive 2000/46 of September 18, 2000 relating to the business of electronic money institutions and their activities (so-called EMD1) and Directive 2000/31 of June 8, 2000 on electronic commerce. The order of July 15, 2009 transposed into French law the payment services directive generating the creation of new institutions offering users a range of services, which are traditionally part of the banking sector. Security constraints have been considerably strengthened because transfers have become extremely easier. Indeed, these new operators affect the historic banking monopoly, whose mechanism was well-oiled and whose authorised operators have high equity capital, combined with security protocols confirmed by use. By necessity, a regulatory adaptation is required. By transposing the directives on service payment and electronic money into French law by order, which is planned in the government agenda for late 2011, France has ***556** nevertheless chosen to focus on an extremely safe and restrictive approach, which does not go necessarily hand in hand with developing an innovative sector.

In the electronic commerce sector, a similar trend is noticeable. This is particularly the case in the specific and highly regulated field of online gaming. The development of the internet has generated particular enthusiasm for this type of game, which was formerly more associated with casinos or bars franchised with the two French operators PMU or FDJ. Again, the practice preceded the law. Only in May 2010 did France choose to liberalise the online gaming industry, which was formerly reserved to the monopolies of the PMU and FDJ operators. Nevertheless, the activity continues to raise important public policy issues. Particular attention has been paid by the legislator to the use of anonymous and prepaid instruments via a trusted third party, which provide cash flow

for gambling.

However, money transfer as well as electronic commerce are at the heart of the current economic considerations. They are part of an increasingly turbulent dynamic, facilitated by the development of new technologies, but affected in their development by their respective legal frameworks.

In the absence of consensus among Member States, France has elaborated an extremely restrictive legal framework designed to control online gambling operators, while maintaining its fiscal resources. This desire for control is exercised, among others, in the control of financial flows and the obligations of operators in the fight against money laundering. These issues are also fundamental in the banking sector.

Having learnt from the crisis intervention or protection of existing monopolies, the reasons put forward by the European and French legislators for imposing such obligations on economic operators are numerous.

This article is not intended to cover all issues raised by the changing economic landscape associated with the currency and the development of the internet. It intends to present the main legal issues raised by the French law in all its complexity facing security requirements on the one hand, and liberalisation of ***557** markets for funds transfer, on the other hand, through the example of the online gaming industry.

## CONTROLLING FINANCIAL FLOWS IN THE FRENCH ONLINE GAMING SECTOR

The control of financial flows incumbent on operators of online gaming is implemented at various levels in the gaming chain of sale. When opening the player's account, the operator must carry out numerous checks, while being obliged to use specific types of payment issuers. Finally, the nature of payment instruments is also subject to regulations.

### Opening a player's account

The player is a central element of control between the financial institutions that make the means of payment available for supplying the player account on the one hand, and online gaming operators that receive funds for the purposes of the game, on the other hand. As such, the player is subject to strict monitoring with respect to the origin of funds and to his identity, whose checks are performed by the online gaming operators. Also, opening a player's account is subject to strict conditions under the Act of May 12, 2010 and its related regulations. Specific regimes are set up. They distinguish a provisional player's account from a definitive player's account.

According to these regulations, the online gaming operator has to identify the players before any transfer of funds from the player's account to the bank account which is held by the same player. It must also obtain communication of his valid ID card and documents proving that the bank account, onto which its assets will be paid, has been opened by the same player within a month. The provisional player becomes definitive, once said documents have been obtained and checked. If the documents have not been received within the prescribed period, the operator must close the provisional account at the end of a period of two months.

The French Regulatory Authority for Online Gaming (known in French as ‘ARJEL’) is particularly attentive to the opening accounts procedure. In the case of subcontracts with respect to the identification process performed by a third party for the online gaming operator, which is usual in practice, ARJEL advocates that the subcontract stipulates clauses ensuring the control and follow-up of the identification process by the online gaming operator. It did not hesitate to initiate an administrative proceeding against an operator who did not perform real-time archiving. According to the authority, the failure observed may lead to the assumption “that the [financial] operations and movements be made in the absence of prior opening ***558** of the corresponding players' account …”. After the ARJEL sanction committee did not impose a penalty on the basis of the alleged statement of objections, the case is currently pending before the Conseil d'Etat (the French Supreme Administrative Court).

Despite the current interpretation debates over these legal texts, it is clear that the regime set up for opening player's accounts is extremely burdensome for online gaming operators. This is also the case in the choice of the

payment instrument issuer.

**The issuer of payment instruments**

The issuer must be a provider of payment services, that is to say a payment company, an electronic money company or credit company authorised by one of the national authorities of the European Union.

These firms are subject to strict regulations and must receive special approval. In France, the national competent authority issuing the approval required for these institutions is the Autorité de contro?le prudentiel (ACP), newly created in 2010.

To date, and only for payment companies, the ACP has issued very few approvals. It favoured a very restrictive interpretation of the Payment Services Directive, transposed into French law by the order of July 15, 2009.

Payment companies can theoretically be formed with a minimum capital of ##20,000 up to ##125,000, depending on the services provided. They are required to choose a method of calculating their own funds which shall reflect the estimated volume of activity planned over a period of at least three years. They must also justify the protection of funds received through bank guarantee or guarantee underwritten by an insurance company. They are also subject to internal control and to the fight against money laundering and terrorist financing in the same way as are credit companies.

The emergence of these new operators can compete with the banking monopoly, in particular by reducing transaction costs and facilitating trade with relatively low amounts, some gambling bets amounting only a few euros.

However, security requirements made by the ACP significantly prevent new entrants from entering into this market.

This concern was recently expressed by Ms Colette Langlade, a member of the French Parliament, in a ***559** written question to the Minister for Economic Affairs on March 15, 2011.

The Minister's response speaks for itself. The Government specifies, of course, that credit institutions are the only institutions justifying sufficient security and solidarity conditions, enabling management of the consequences implied by the adhesion to the clearing bank system. However, discrimination and constraints are expressly recognised:

“However, given the barriers to innovation and obstacles to the development of competition in the payments market to which the exclusion of payment institutions may eventually lead to, a French Committee for Banking Standards organisation (CFONB) was put into place in order to identify solutions to facilitate the processing of payment orders for customers of payment institutions from payment systems under conditions of transparency and strengthened traceability.”

In France, the Electronic Money Directive ( so called EMD2) was originally expected to be transposed into French law by April 30, 2011. But its transposition was postponed to no earlier than late 2011. In any case, it did not allow new operators to enter the French market. Indeed, the 2000 EMD1 is too restrictive, in particular with respect to the maximum amounts of rechargeable instrument. Then the capital requirements are as strict as those applicable to credit institutions. In theory, however, the directive is directly applicable and may be opposed to the ACP. In practice, it is likely that the Authority wait for its transposition by order.

As a result, new agreed institutions are most often credit institutions or affiliated to trusted third parties with majority stakes in institutions benefiting from approval by another national competent authority in Europe. This is the case of Paypal, which makes use of the European passport to operate in France.

Although the issuer to supply the player account is broadly defined in the French Online Gambling Act of May

12, 2010, the current system is based solely on the traditional banking system, including online payment.

In terms of the nature of the payment instruments, however, the player has more options at his disposal.

**The nature of the payment instruments**

Instruments of payment for the supply of the player account are specifically defined in the online gaming ***560** legislation. Thus, art.17, para.6 of the Act of May 12, 2010 provides that:

"the supply of a player account by the holder can be achieved only by means of payment provided by a payment service provider established in a Member State of the European Community or a State Party to the Agreement on the European Economic Area which has concluded an agreement with France containing an administrative assistance clause in the fight against fraud and tax evasion. Only payment instruments mentioned in Chapter III of Title III of Book I of the Monetary and Financial Code can be used."

Many payment instruments can be used by the player to fund its account managed by the online gaming operator. Indeed, payment cards, regardless of the mode of flow, bank transfers and payments made through the intermediary of a trusted certified third party are authorised.

By contrast, the following payment instruments cannot be used: coins, bank notes, bank cheques and postal orders, or bills of exchange. Such exclusions do not affect the gaming industry proposed outside the internet, where cash payment is for example possible. This exclusion seems to be justified by the legislator because of the nature of opening and functioning of a 'cyber' account, these payment instruments remaining under the banking competence exclusively.

In this context, electronic money acquires a very new dimension. Indeed, in the marginal hypothesis where the player prefers to hide his activity both to his banker and to his entourage, the prepaid card is the preferred payment. Indeed, he will not be asked to communicate bank details or for access to its assets in case of addiction and/or massive loss.

On this point, parliamentary discussions were very lively. Allowing the player to use a payment instrument with anonymous characteristics raises questions about security in terms of fund traceability.

The current regulation, however, authorised a relatively low amount to be charged on this type of instrument. It aims at preventing bets of substantial amounts or funds transfers of dubious origin, thus allowing a relative flow traceability. The new electronic money directive will still load up to ##250 instead of ##150 today for media which are non-rechargeable, and up to ##2,500 for the total amount of transaction in a calendar year if the instrument can be recharged.

***561** In addition, the player must notify the game operator of his bank account details to which his potential gains will be transferred.

Moreover, Recital 13 of Directive 2009/110 states that:

"The issuance of electronic money does not constitute a deposit-taking activity pursuant to Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, in view of its specific character as an electronic surrogate for coins and banknotes, which is to be used for making payments, usually of limited amount and not as means of saving."

If vulnerabilities appear in terms of traceability, prudential regulations applicable to issuers, however, allow adjustments.

Article 7.3.3 of the French online gaming regulation (cahier des charges) provides, for example, that the opera-

tor must by closing the player's account immediately repay the account holder to pay the credit balance. In cases of suspected money laundering, the operator must defer repayment pursuant to art.L.561-16 of the French Monetary and Financial Code. This obligation results also from EMD2. Its art.11 provides that:

"Member States shall ensure that issuers of electronic money redeem at any time and at his nominal value upon request of the electronic money holder the value of the electronic currency held."

Thus, if online gaming operators are entitled to hold cyber accounts supplied by the players for the purpose of gambling, funds deposited in these accounts cannot in any way be made available to holding companies, or generate interest. Similarly, gaming operators are not entitled to lend to players.

It is also stipulates under art.30 of the Act of May 12, 2010 which states that:

"… gambling on credit is prohibited. It is forbidden for any gaming operator approval holder referred to in Article 21 and any director, officer or employee of such an operator to lend money to players or to set up direct or indirectly ***562** features allowing players to lend money to each other."

The regulation goes further by prohibiting online gambling operators to include on their site advertising links to a financial institution, which may grant credit or promote the activity of credit.

But control obligations to which operators are subject also concern other areas. In fact, to achieve the objective of fighting against money laundering and terrorist financing, the gaming industry, more than any other, is subject to strict prudential requirements. These requirements are similar to those applied to electronic money institutions as well as to payment and credit institutions.

## FIGHTING AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering and terrorist financing are often part of an international context. Gaming in an online environment may also allow players to be difficult to identify. Players may be likely to falsify their identity and to inject funds with dubious origin, which could seriously damage the financial system in particular.

However, the statement of activity of ARJEL states that taking into account all activities, ##1,023 millions were deposited into players' accounts since the opening of the market, including e509 millions in the first half of 2011. The Online Gaming Act of May 12, 2010 which legislates in an area which may be linked to money laundering risks, and the effect on the volume of trade are sufficient to justify the establishment of strict control.

The law refers several times to the requirements imposed on operators; an operator shall:

"justify its ability to meet its obligations in the fight against the fraudulent or criminal activities, particularly money laundering and terrorist financing".

Chapter VI of the Act is devoted to issues including the fight against money laundering. Article 22 refers to the French Monetary and Financial Code. Article 23 imposes an obligation on the operator of annual certification, including security proceeding controls in both computer and legal matters.

### The player identity

The first control consists in verifying the player identity when the operator opens the player account. Thus, ***563** art.L.561-5 of the French Monetary and Financial Code requires online gaming companies to identify their clients and, if applicable, the beneficiary of the business relationship. If the company is unable to identify its customer, it must refuse any transaction.

Directive 2005/60 of October 26, 2005 on the prevention of the use of the financial system for the purpose of

money laundering and terrorist financing sets the harmonised rules at Member State level. Recital 14 specifies that "this Directive should also apply to those activities of the institutions and persons covered hereunder which are performed on the Internet."

This directive was transposed into French law by order of January 30, 2009, codified in the French Monetary and Financial Code.

Pursuant to art.L.612-14 of the Monetary and Financial Code, the ACP Supervisory Board, by a decision of May 28, 2010, as amended June 21, 2010 and March 23, 2011, created an advisory committee dedicated to the "fight against money laundering". This committee is responsible for advising on all documents concerning the fight against money laundering and terrorist financing before adoption by the ACP Supervisory Board. It is consulted on intended investigations concerning information submitted by agencies which are under the control of the ACP in the fight against money laundering and terrorist financing matters. This information may result from documents delivered periodically or from the sample as completed in the approval process or from any other authorisation process.

The provisions laid down by the ACP are methodologies to be applied similarly in the online gaming sector, where the regulation is comparable.

Pursuant to art.L.561-2 9o bis of the Monetary and Financial Code, the obligations relating to the fight against laundering and terrorist financing shall be implemented by "legal representatives and managers responsible for gaming and betting operators allowed on the basis of Article 21 of Law No.2010-476 of 12 May 2010 relating to the liberalisation and the regulation of online betting and gambling." Pursuant to the rest of the list set out under this article, this shall also apply to "credit, payment and electronic money institutions".

Specifically, online gaming operators should put into place proceedings for monitoring clients' identities and the nature of the funds transferred to players' accounts. Each year, online gaming companies are also audited internally by a third party accredited by ***564** ARJEL with the view to verifying whether the procedures in place are respected and functional.

**Suspicious Transaction report (STR)**

Online gaming operators shall also report suspicious transactions according to art.L.561-15 of the French Monetary and Financial Code.

The procedure for payment institutions is detailed in the CECEI instruction, the Banking Commission (now called ACP) No.2010-08 of March 8, 2010, and its appendices. The gambling regulation (cahier des charges) dated May 17, 2010 also states that gambling operators should implement procedures:

"to meet the following requirements:

-- its obligations in terms of due diligence;

-- its obligation to report to Tracfin--the French state unit for intelligence processing and action against illicit financial networks--transactions which are known, suspected or be reasonably held to be suspected for being part of a money laundering or terrorist financing scheme;

-- its procedures and its internal control system (assessment and risk management information and regular training of its staff), in reference to Title VI of Book V of the Monetary and Financial Code."

The fight against illegal sites illustrates also the strict control over fund transfers in the online gaming industry.

Given the risks via gaming, it is clear that internal control procedures, although these are not as strict as those

applying to financial institutions, must be put into place efficiently. In practice, operators shall pay particular attention to ACP's circulars and doctrine. ARJEL also works closely with stakeholders in the fight against money laundering and against terrorist financing, including the ACP but also the AMF--the French public authority tasked with investor protection--and TRACFIN.

Moreover, in a decision dated February 24, 2011, ARJEL reminds the online gaming operators of their obligations in terms of procedures and internal control measures with a view to fighting money laundering and the financing of terrorism. It prescribed a number of recommendations and establishes a risk analysis of the sector for operators.

This doctrine is a real guide for authorised operators, referring to the provisions of the French Monetary and ***565** Financial Code, while adapting its operational requirements to the specificity of the online gaming sector. It is largely inspired by the general regulations. Operators can refer to the ACP's circular on the subject for the development of their internal procedures.

However, as the player accounts being supplied by payment instruments issued by financial institutions are themselves subject to strict requirements, it may be hoped that the reconstruction of the transfer of funds is fully traceable. The online nature of gaming also helps to prevent payment by cash or the traditional activity of casinos. The system developed should prove itself.

## CONCLUSION

At a time when banks are getting closer to the French historic phone operator--France Telecom--in order to offer to its customers m-commerce (payment by mobile phone), at a time when phone operators are becoming partners of computer companies to offer ultra-secure and user-friendly systems dedicated to money transfer, at a time when developing countries spread the NFC technology in order to replace a system without a banking system and characterised by micro-payments, at a time when American net giants launch their applications for electronic portfolio and internalise payment systems to their own business, at time when a severe financial crisis has affected confidence in the traditional banking system, the world has witnessed a profound transformation of the economic system of trade. This transformation can, in some way, be compared with the revolution at the time of the emergence of the railroad during the industrial era.

But money transfer control and the fight against money laundering and terrorist financing may not constitute the risks which are more likely to be realised in the technology sector. The emergence of new banking operators and the complexity of security-related issues at this time and computer techniques reveal a potentially higher risk due to cyber-crime. It is also the lack of trust in certain technologies, including mobile terminal equipments, which prevents a greater development of paperless payments. What about the opportunity to play at any time online via a mobile phone technology that may facilitate hiding or falsifying identity? What about computer hacking allowing intrusion into player accounts or fund interception? The analysis of legal mechanisms put into place suggests that vulnerabilities exist side by side with the new technologies and require consumers be protected accordingly.

***566** This natural distrust should not, however, prevent the sector of online money transfers from developing, which is necessary adaptation for economic exchanges related to the changes in the internet to the 21st century. The French legal system which is extremely protective has chosen to liberalise the French gambling market previously in the hands of state monopolies, while preventing new innovative operators from entering the French market, to the benefit of the greatly disparaged banking monopolies. It can only be hoped that this schizophrenia leads to a de facto liberalisation of the e-money market and to online gaming regulations at Community level, so that the European consumer can be protected in an appropriate way.

## PERSPECTIVE OF AN EXPERT IN COMPUTER SECURITY: INTERVIEW WITH MR. CYRILLE BARTHELEMY

**1. Question: The security of fund transfers is subject to restrictive legal regulations, which seems to be**

**combined with technological constraints. What do you see as the main security problems posed by online payment?**

**Answer** : The proliferation of actors involved in the origin or in the treatment of cash flows lead to a growing complexity of their security.

Particular attention should be paid to offset operations on the internet, such as e-commerce transactions between banks, customers, payment operators, or between clearing houses. Highly regarded targets are, for example, stored or transferred bank data, virtual portfolios--including virtual currency such as Bit-Coin--payment information and technical means allowing interaction with the banking systems.

In the particular case of mobile computers, of mcommerce and of Near Field Communication, much remains to be built in terms of security.

2. **Question : To what extent do you think that these vulnerabilities prevent the present development of economic sectors with strong online cash flows, such as the online gaming industry?**

**Answer** : Indirectly, through the constraints imposed by legal regulations, these vulnerabilities represent a ***567** financial or organisational brake on the emergence of new entrants, who are potentially innovative, but have a priori smaller means at their disposal to implement security measures.

In addition, as was the case at the beginning of the ecommerce development, the primary criterion is building trust. However, recent news concerning piracy may be considered to be an obstacle or as a trigger for action.

**3. Question : What are your recommendations for addressing potential security vulnerabilities?**

**Answer:** First, educating all stakeholders with an appropriate speech.

Secondly, applying pragmatic security basics. The topic has to be considered as a process and to be thought about upstream without reducing the debate to a technical problem or to a constraint: (i) What should be protected? (ii) How to do it appropriately, to take full advantage of it and how to control it?

Risk analysis and evaluation of the actual level of security can anticipate security vulnerabilities, which may be costly both financially and in terms of confidence.

Avocat au Barreau de Paris, Certificateur juridique agréée par l'ARJEL au sein du groupement Intrinsec/ **Le More**/RSM Rsa depuis 2010.

Avocat au Barreau de Paris et spécialiste en matière de paiements dématérialisés.
END OF DOCUMENT