Technical note on fraud management in gambling operators

CONTENTS

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

1. Introduction

The fight against fraud is one of the cornerstones of Law 13/2011 of 27 May on gambling regulation (Law 13/2011 or LRJ) and a consequence of establishing a regulatory framework for the national level gambling activity offered through the corresponding licence. In this sense, establishing systems and mechanisms to prevent fraud and money laundering is an express obligation in the licence to offer national level gambling activities, specifically in the various general licences held by the operators.

The Directorate-General for the Regulation of Gambling (DGOJ) necessitates that operators include a suitable policy to analyse fraud and manage detected risks in their strategy and operating procedure. Thus, since 2017, the terms and conditions of all new licence requests have included the requirement of the operator to produce a fraud manual which details the procedures and measures implemented to identify fraud scenarios and how they are handled[1]. Enshrining this requirement at a legislative level is planned in the near future.

Proper risk management of fraud in gambling is based on appropriate initial identification of the risks to which the operator is exposed. The assessment of fraud risks shall lead to systematic prevention measures being established that prevent them and detect them and which allows cases of fraud to be found when they occur as well as determining corrective actions to help and ensure a potential fraud is appropriately and quickly addressed. Finally, all fraud management tasks shall be measured and documented in assessment reports.

This document analyses the main types of fraud identified by the DGOJ which a gambling operator may witness, the structural measures of prevention and detection set out in regulation or instructions of the Directorate General, the qualified risk scenarios which must be taken into account to protect the rights of gamblers with a specific focus on vulnerable groups, as well as possible actions to take in managing alerts, as appropriate.

The document's purpose is to assist the gambling operator by pointing out the minimum content that, notwithstanding the specificities applicable to each organisation, can be considered from the standpoint of end-to-end fraud management by licensed operators, affording assuredness on that which the Directorate General understands as diligent fraud management.

Experience obtained from developing gambling activities in a regulated and controlled environment since 2012 has allowed us to know and become aware of the various types of fraud which could occur on gambling platforms. From analysis of the information available to us - user records and gambling transaction data supplied by the operators, information in the case files, and partnership actions with state security forces - it is evident that the main fraud risk on gambling platforms is

[1] Section four of the Terms and Conditions of the general licence states "*The holder of the general licence will have the systems and mechanisms in place to avoid and prevent fraud and money laundering on the terms set out in the Fraud Prevention Manual, the Operating Plan and the Technical Gambling Systems Project supplied with their licence request as well as the prevention procedure manual submitted alongside the licence request and modified pursuant to the observations of the Executive Service of the Commission for the Prevention of Money Laundering; and without prejudice to the need to comply with the instructions of the Directorate-General for the Regulation of Gambling, the aforementioned Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences and other competent bodies.*"

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

impersonation, consensual or not. These practices try to circumvent the access controls established by operators, so, notwithstanding being the channel for other types of fraud, could be being used by people who are banned from gambling such as minors, people with gambling problems registered in the RGIAJ[2] or who have excluded themselves from the operator, people linked to the operator or people linked to the sport. The use of a third-party's identity data to open a gambling account or the assignment of use of the gambling account may be the means employed by "fixers" of sporting events to profit from betting. Other, albeit lower incident, risks but also with a high impact on people and gambling activity are the use of cards or other payment methods by others, the use of other people's money or money of which the origin cannot be proved for gambling or the use of privileged information to gain advantages over other gamblers.

This document analyses these different types of fraud and establishes a two-level control system to identify existing risks and the operator's reaction to them.

Level 1 is a set of measures which has to be adopted and implemented by all gambling operators and which are transversal across all gamblers. In some cases, the instructions are developed with a high level of detail through gambling regulation. In other cases, qualified risk scenarios are defined, i.e., specific and identifiable patterns observed in gambling activities which potentially have a greater probability of being fraudulent. The operator shall analyse these qualified risk scenarios to specify their own measures and procedures based on this document and their own knowledge and experience.

Level 2 is made up of the guidelines that shall govern operators' fraud management systems in terms of the appearance of possible risks which occur. This level sets an exhaustive list of risk scenarios and the measures to take to clarify the facts and ultimately act against the fraud when confirmed.

Given the importance of this to all actors in the gambling market, regardless of their being public or private, this document aims to set a frame of reference to help operators implement their own fraud risk management system which fully complies with applicable regulation in any event. We understand that this frame of reference must be viewed as a living framework that continually has to adapt to the specificities and peculiarities of fraud in the online gambling market, which is an activity subject to constant evolution and innovation.

2. Types of fraud in online gambling

A. Identity data fraud

1. CONTEXT

We consider identity data fraud to be those practices consisting of:

[2] General Register of Gambling Access Bans

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

A. Attempts to register with correct identity data but altering some, usually age.

This type of identity data deceit may be used to circumvent the access controls on minors set by the DGOJ and the operators. Any alteration to identity date - DNI/NIE, name, surname or age - is automatically detected by the DGOJ's gambler identity verification system and communicated to the operator so the registration process can be blocked.

B. User registration with third-party data or assignment of use of a verified user record.

This identity data deceit may be used to circumvent the gambling or access controls set by the operators in dealing with different motives. By way of example, some of these motives include:

- ✓ People banned from gambling pursuant to article 6.2) of Law 13/2011 such as minors, problem gamblers registered in the RGIAJ or those who have excluded themselves from the operator, people linked to the operator or people linked to the sport.
- ✓ People having direct or indirect knowledge of a future fixed sports results and bet to make a profit.
- ✓ People previously blocked by the operator when applying their fraud prevention policies.
- ✓ Gamblers who are considered as having special skill in betting and "share" that knowledge with third parties who also assign the management of the gambling account to them, in exchange for some form of compensation.
- ✓ Gamblers who wish to make bets above the level accepted by the operator and use various accounts to bypass the controls.
- ✓ Gamblers who seek to take advantage of the welcome bonus advantages offered to new customers by the operators on multiple occasions.
- ✓ Gamblers who seek to avoid paying the Income Tax on winnings.

In these cases, the use of third-party data may be consensual or not.

We speak of consensual impersonation when it is known and not reported; It usually occurs in a family environment or with friends or third parties who hand over the identity data in exchange for some form of compensation that can be received on one occasion or periodically following a "gambling account rental" model. In this last model, the lessor of the account corroborates its authenticity with the operator's different controls or those of the bank when also assigning use of the means of payment associated with the registry.

We speak of non-consensual impersonation when it is not known by the owner of the identity data. In these cases, the means of payment used may be anonymous or not, making use of third-party cards. Included within this group is using the identity of deceased people.

The proper management of the fraud risks is broken down in two levels. The qualified risk scenarios identified by the Directorate General are described and the measures that must be implemented by the gambling operators are established for each level.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

2. LEVEL 1 CONTROLS AND ACTIONS RELATED TO IMPERSONATION

The following measures are part of level 1 for the prevention of impersonation[3]:

2.1. Gambler identity verification

The gambler identity verification process collates the information in the user record and verifies the truthfulness of the data supplied. It includes the following control measures:

a) The gambler filling out a registration form with the data required under gambling regulation.

b) Checking the truthfulness of the DNI/NIE, name, surname and age data supplied. This verification can be performed through the identity verification web service provided by the DGOJ.

c) Check that there is no registration in the gambling ban register through the RGIAJ verification web service provided by the DGOJ.

d) Review possible errors in the entered data such as streets or postcodes that do not exist, there being no match between the postcode and the city of residence or between the postcode and the tax residence code.

e) Check that a gambler has not registered with the operator after their date of death.

2.1.1. Risk scenarios in the identity verification phase: vulnerable groups

a) Registration attempt using the identity or connection data - name and surname, address, telephone number, email, IP address, device identifier or other identity or connection data - coinciding with those of a failed registration attempt of a minor[4].

b) Registration attempt using the identity or connection data - name and surname, address, telephone number, email, IP address, device identification or other identity or connection data - coinciding with those of a person registered in the RGIAJ or who has excluded themselves from the operator.

c) Registration attempt using the identity data of deceased people[5]. After the operator has blocked the account, there are registration attempts using some of the identity or connection data -

[3] Articles 26 and 27 of Royal Decree 1613/2011 of 14 November, developing the technical requirements of gambling activities under 13/2011 of 27 May on gambling regulation and its implementing regulation.

4 On 14 November 2018 the DGOJ launched new enhanced functionality of the gambler identity verification service that allows the operator to know the registration attempts in which a DNI associated with a minor has been used where any of the identity or age data during the registration process has been modified. To date, when the system detected an error in the identity data it gave the message "data with errors" but did not give details on the error. This enhanced functionality allows operators to know when a verification process error is due to registration attempts with the DNI of a minor. With this information, they shall include additional controls to detect the possible reuse of the same identity or connection data of that registration attempt - name and surname, address, telephone number, email, IP address, device identifier - to prevent future access attempts using other identities.

5 On 14 November 2018 the DGOJ launched new enhanced functionality of the gambler identity verification service to include information on the user records whose identity data matches deceased people as recorded in the deceased persons section of the Civil Registry. With this information, the operator may prevent the new registrations with identity data matching a deceased person and, in relation to its historical database of users, shall adopt the appropriate measures in accordance with the provisions of article 33.2 and/or 35.3 of Royal Decree 1614/2011, of 14 November, which develops Law 13/2011, of 27 May on gambling regulation, in relation to gambling licences, authorisations and registries, without prejudice to the remaining provisions that apply in civil law.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

name and surname, address, telephone number, email, IP address, device identifier or other identity or connection data - coinciding with those of a deceased person or those of the registration attempt.

2.1.2. Risk scenarios in the identity verification phase: duplicate accounts

d) There is an active account associated to the same identity data - DNI/NIE, name, surname and age -.

e) There are several user records with matching identity data - name, surname and age - but different documents corresponding to people who register several times with the same operator using their DNI, NIE and/or passport.

f) Several user records have been created sequentially from the same device and IP address in a short space of time using different identity data although normally sharing the same telephone and/or email address.

2.1.3. Actions to take in the described scenarios

Move to the document verification phase

2.2. Gambler document verification

Gambler document verification allows the truthfulness of the identity data provided by the gambler in the user record to be verified by requesting genuine documents.

The purpose of checking identity data through documents is to ensure that the identity given by the participant corresponds to the real identity. The checking process involves obtaining a copy of a valid document and, to the extent that it is possible, check that it has not been altered and that it truly belongs to whomever submitted it.

As established in the Resolution of 12 July 2012, which approves the provision that develops articles 26 and 27 of Royal Decree 1613/2011, of 14 November regarding the identification of the gambling participants and the control of the individual prohibitions to participating, modified through the Resolution of 31 October 2018, of the Directorate-General for the Regulation of Gambling, by which certain resolutions on gambling activities provided for in Law 13/2011, of 27 May on gambling regulation are modified, gamblers not verified through documents can only deposit a joint limit of up to 150 euros and participate in gambling but may not withdraw the prizes.

2.2.1. Actions to take in the document verification phase

Check that the document supplied belongs to the person identified in the registry.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

It can be done using different procedures from the gambler sending a photograph holding their original document to that which also allows the comparison of their face with the photograph attached to said document, right up to applying a full digital identity verification procedure (digital onboarding).

Digital Onboarding is understood as the remote identification process that allows users to register as new customers in a fully digital manner. Several digital onboarding tools have appeared on the market that include advanced features such as[6]:

1. Automatic user registration processes.
2. Automatic document identification.
3. Checking the veracity of the documents' authenticity.
4. Extracting the biometric and alphanumeric data from the identity document.
5. Contrasting the photo in the identity document with the image of the person.
6. Proof of life.
7. Videoconference.
8. Mobile phone number validation.

The following risk scenarios are established in this general obligation.

2.2.2. Risk scenario in the document verification phase

g) There are doubts as to the veracity of the identity documents supplied such as forgery or manipulation.

h) There are doubts as to the match between the document's holder and the actual person who registered.

2.2.3. Other possible actions in the scenarios described, according to the case

- Repeat the identity document verification process.
- Request new documents from the gambler: new identity document, copy of utility bill (electricity, water or other), etc.
- Make telephone contact: telephone call or videoconference.
- Validate the gambler's mobile phone number by sending an SMS.
- Validate the gambler's email address by sending a message with a verification link.
- Validate the gambler's address by sending a letter.

6 In the framework of checking the authenticity of documents, there are standards in the industry such as ICAO 9303 or ISO/IEC 7501-1. In the context of facial recognition, there are benchmark algorithms evaluated by NIST (National Institute of Standards and Technology).

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

3. LEVEL 2 CONTROLS AND ACTIONS RELATED TO IMPERSONATION

3.1. Active monitoring of the relationship with the gambler

Once level 1 has been completed, level 2 comes into play. Appropriate management of impersonation risks requires additional control measures during the contractual relationship with the gambler to detect those cases of fraud in the identity data that could not be detected at registration. This level mainly consists of active monitoring of gamblers and shall be a dynamic relationship under constant review for possible qualified risk scenarios.

3.1.1. Risk scenarios during the gambling activity

i) Gambling activities take place - deposit, participation or withdrawal of funds - using a gambling account of a deceased person after their date of death.

j) Attempts to unblock users who are blocked by registration in the RGIAJ or by self-exclusion in services in which the operator's staff intervene directly.

k) There are several claims of similar content filed by a set of gamblers sharing identity, address, telephone, email address, device or IP address information.

l) There is gambling activity from users of an advanced age whose gambling behaviour is atypical to the type of gambling, the time gambling is done or the intensity of the activity.

3.1.2. Actions to take in the described scenarios

In i) there is a clear indication of the use of identity data by a third party.

In j), k) and l) it will be necessary to confirm the gambler's identity using the actions to correctly verify their identity as described above. The choice of the specific measure to use will depend on the specific case and the information available.

4. UNILATERAL TERMINATION OF THE CONTRACT AND COMMUNICATION TO THE DGOJ

Where proven that the gambler has committed identify fraud or has allowed their data to be used by third parties, the operator may invoke article 33.2 of Royal Decree 1614/2011 of 14 November, implementing Law 13/2011 of 27 May on gambling regulation in relation to licences, authorisations and gambling registers.

B. Means of payment fraud

1. CONTEXT

Means of payment fraud is the use of a means of payment by the gambler, mainly cards, in another person's name. This type of fraud may be consensual or not.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

We refer to consensual means of payment fraud when the titleholder of the means of payment is aware of it. At times, the use of another person's card is accompanied by the subsequent disavowal of the transactions made.

We refer to non-consensual means of payment fraud when the holder of the titleholder of the means of payment is unaware of it. It is normally reported to the police at the time the holder becomes aware of the unauthorised use of the card.

There is a two-level control system in place.

2. LEVEL 1 CONTROLS AND ACTIONS RELATED TO MEANS OF PAYMENT

2.1. Traceability of transactions

Within the means of payment fraud risk management policy, the operator must ensure that all transactions are fully traceable. In analysing and managing the fraud, the operator will pay special attention to means of payment whose title cannot be immediately identified or verified. Verifying the means of payment is the process through which the means of payment's holder's data is obtained[7].

In general, taking the following criteria into account shall be appropriate:

- Withdrawals of funds from the gambling account will be through the same means of payment used for the deposit[8], provided that it allows traceability. Otherwise, the withdrawal must use a traceable and verified means of payment.
- In particular, if the means of payment used in the deposit is anonymous, withdrawals will be through a means of payment that is traceable and verified (e.g. by bank transfer or by card when it has been verified).
- The intention is to minimise the number of different means of payment used by gamblers.

2.1.1. Risk scenarios

a) Attempt to withdraw funds from a gambling account with an anonymous means of payment.

b) Attempt to withdraw funds from a gambling account with a means of payment which differs to that of the deposit while the means of payment is nominal but not verified.

2.1.2. Actions to take in the described scenarios

Withdrawals of funds using an anonymous means of payment are not permitted.

[7] To ensure the traceability of the transactions and aid any subsequent means of payment fraud investigation, the operator must retain the verified means of payment's holder's data and the last four digits of the account or card; or have the mechanisms to obtain them should they be requested by the competent Spanish authorities.

[8] Article 38, section 1 of Royal Decree 1614/2011 of 14 November which develops Law 13/2011 of 27 May on gambling regulation in relation to licences, authorisations and gambling registers.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

Withdrawals of funds using a means of payment different to that used for the deposit are not permitted until it has been verified as belonging to the holder of the gambling account.

3. LEVEL 2 CONTROLS AND ACTIONS RELATED TO MEANS OF PAYMENT

3.1. Active monitoring of the relationship with the gambler

Appropriate management of means of payment fraud risks requires additional control measures during the contractual relationship with the gambler to detect those cases of fraud which had not been possible to detect using the measures at level 1.

3.1.1. Risk scenarios for means of payment

c) Request to withdraw funds without any gambling activity having taken place.

3.1.2. Actions to take in the described risk scenarios

The request to withdraw funds from the gambling account without any gambling activity having taken place or with minimal activity in relation to deposits requires the specific circumstances to be analysed to rule out possible fraud.

4. UNILATERAL TERMINATION OF THE CONTRACT AND COMMUNICATION TO THE DGOJ

Where proven that the gambler has committed means of payment fraud, the operator may invoke article 33.2 of Royal Decree 1614/2011 of 14 November, implementing Law 13/2011 of 27 May on gambling regulation in relation to licences, authorisations and gambling registers.

C. Source of funds fraud

1. CONTEXT

Source of funds fraud is the gambler's use of stolen money, money which the user is not authorised to have or use for said purpose, or money whose source cannot be proven.

2. LEVEL 1 CONTROLS AND ACTIONS RELATED TO SOURCE OF FUNDS

2.1. Verification of the gambler's economic capacity

Checking the gambler's economic capacity in relation to their level of spending aims to confirm that the funds used belong to them[9].

[9] Checking the gambler's economic capacity is also an element to consider in the operator's responsible gambling policy as it also serves to prevent gambling with third-party loans.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

Within the source of funds fraud risk management policy, the operator must define the assumptions under which, in any event, the gambler's economic capacity will be checked.

2.1.1. Risk scenarios in the checking the economic capacity phase

a) An annual cumulative volume of deposit equal to or greater than 36,000 euros.

b) Users rated as “VIP” customers. Gamblers rated as “VIP” users require monitoring of the grounds for that category and checking that they aren’t using funds which aren’t theirs.

2.1.2. Actions to take in the described scenarios

Verification of the gambler's economic capacity can be carried out by any generally accepted means of evidence, for example asking the gambler for documents supporting their solvency (payroll, employment history report, income tax declaration, etc.).

D. Geolocation fraud

1. CONTEXT

Geolocation fraud, in the context of gambling activities, is the use of virtual private networks (VPNs) or proxies to hide the IP address of the device to hide the location in Spain of the gambler. The reasons for these practices are varied:

- Persons attempting to bypass the identity controls established by the operator on the ".es" platform for any of the reasons described in point 2.A of this document.
- People attempting to avoid the traceability controls on transactions for tax reasons.

These practices may affect gambling operators who, directly or through their parent companies or subsidiaries, operate in other jurisdictions.

2. LEVEL 1 CONTROLS AND ACTIONS RELATED TO GEOLOCATION

2.1. Controlling the gambling on offer

The operator, who directly or through their parent companies or subsidiaries, operates in other jurisdictions, must implement measures that, as far as possible, detect and prevent connections from users located in Spain who try to access their gambling platforms other than those authorised by a Spanish licence using network technologies whose purpose is to hide their IP address.

2.1.1. Risk scenarios in the checking the gambler’s location phase

The main problem to correct geolocation comes from the providers of proxy and VPN services and therefore geolocation never 100% guarantees the user’s location.

2.1.2. Actions to take in the described scenarios

constitución

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

Firstly, the operator can maintain lists of publicly known proxy or VPN IP addresses. This way, a gambler connecting from one of these IPs can be an indication that the gambler's real location is not that of the connection IP, requiring additional checks with other sources to confirm the gambler's location.

To increase the number of cases with gamblers' geolocation being correct, gambling operators can implement additional IP geolocation services or contrast the gambler's IP with geolocation databases. There are commercial solutions which facilitate geolocation. The choice of tool will depend on the data you wish to know about the IP, the type of service required (verification by HTTP request, geolocation database, etc.) and its accuracy.

In addition, for mobile applications, IP geolocation can be complemented with physical geolocation (GPS, Wi-Fi, mobile networks in range, etc.).

In any case, the use of geolocation tools must be complemented with additional control measures based on identity data, residence data and means of payment used, as well as applying procedures to detect fraud. At times, the companies which offer geolocation tools, also offer anti-fraud tools.

E. Fraud in bets linked to fixed sports events

1. CONTEXT

The threat of fraudulent bets linked to a sporting event being fixed is a complex issue to analyse and has a cross boarder nature as it can affect any sport and sports competition with fraudulent bets being made with betting operators of any jurisdiction.

Fraud in bets linked to fixed sports events is the use of bets to benefit from knowing that a certain event or sporting event has been previously fixed.

The complexity of the environment surrounding sports betting requires the continuous and joint effort of all stakeholders to identify vulnerabilities, take preventive and dissuasive actions and establish mechanisms to detect and prosecute with the aim of preventing integrity in sport from being compromised and that, if it occurs, those involved can be identified.

2. LEVEL 1 CONTROLS AND ACTIONS RELATED TO FIXING

2.1. Preventive actions

2.1.1. Training

The main line of prevention is training. It is up to each stakeholder, within their area of competence, to work in sharing the message stating the risks of fixing a sports event or betting having knowledge of it, as well as clearly informing of the consequences of fixing and betting with knowledge of fixing having taken place.

constitución

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

This action can be carried out in multiple forms: workshops, messages, leaflets, advertising campaigns, manuals, announcements, informative notes, etc. Each stakeholder will assess which strategy best suits their objectives.

2.1.2. Obligations regarding information

The fight against fraud in bets linked to the fixing of events is based on sharing information with a dual purpose; on one hand, to inform stakeholders of the existence of atypical situations that could possibly indicate fixing and, on the other, build the necessary intelligence to fight this increasingly sophisticated type of fraud.

Sharing information about possible fixing must occur at least at the following levels:

- With Spanish Law Enforcement Agencies regarding possible crimes.
- With the DGOJ regarding alerts to possible fixed events.

The generation of "intelligence" among all stakeholders is fuelled by exchanging knowledge, research techniques and procedures, best practices, etc.

2.2 Detection actions

Detection actions are based on monitoring bets to detect anomalies and their subsequent analysis and investigation. These anomalies, although not in themselves constituting evidence of fraud in a certain event, are an alert about irregular[10] or suspicious[11] betting.

The analysis of the alerts relating to fixed sporting events must include the degree of them based on the confluence of indications. In short, unless there is evidence or confluence of many indications, an alert is strictly atypical behaviour of the betting market that cannot be explained.

Detection actions must also contemplate what described in the identity and means of payment fraud sections, given that a usual practice is for bets linked to fixing to be placed making use of multiple false identities, thereby bypassing the operator's controls and concealing the benefits.

Once the alerts detected by the betting monitoring system have been analysed, they must be communicated to the DGOJ which manages the national alerts system.

3. LEVEL 2 CONTROLS AND ACTIONS RELATED TO FIXING

[10] Irregular sports betting: any sports betting activity inconsistent with usual or anticipated patterns of the market in question or related to betting on a sports competition whose course has unusual characteristics. Source: Macolin Convention.

[11] Suspicious sports betting: any sports betting activity which, according to reliable and consistent evidence, appears to be linked to a manipulation of the sports competition on which it is offered. Source: Macolin Convention.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

3.1. Active monitoring of the development of events and bets made

Within the fraud related to fixing risk management policy, the operator must define the assumptions which will generate a warning subject to analysis and reporting to SIGMA[12].

3.1.1. Risk scenarios in the analysis of user registrations

a) Registration of users who are prohibited from accessing gambling under the provisions of article 6.2) of Law 13/2011 and, in particular, persons linked to the operator or persons related to the sport which the operator knows.

b) Registration of users with the same login, email address and even initial deposit patterns. Multiple user records with matching data such as phone, email, device or IP address.

c) Several user records created in a short space of time with address data in a very concentrated geographic area - even in the same block of buildings.

d) Several unsuccessful verification attempts with the same identity data, but varying DNI, dates of birth or name variants (i.e.: Mike Smith, Michael Smythe, Mick Smithe).

e) Use of email accounts created on servers with end-to-end encryption. The use of email accounts whose main characteristic is end-to-end encryption prevents the account provider from accessing the content of these emails which makes the traceability of operations difficult in cases of police investigation.

f) Use of "disposable" email accounts that disappear in a few days whose main purpose is to avoid excess advertising or spam mails, but which can also be used to hide real identities.

g) User accounts opened on dates immediately prior to an event to specifically bet on it.

h) New accounts opened in the same area or region, especially if the region in question can be associated with one or more of the participants in an event.

i) There are indications that the account is under the control of a third party. For example, the account is in the name of a woman, but the email address is in the name of a man.

3.1.2. Risk scenarios in analysing the form of gambling

j) Gambling accounts used specifically for an event after being inactive for a significant period of time since its opening.

k) Bets showing that the gambler does not have normal monetary management; for example, the full account balance is gambled or bets at any price.

l) Users who use all the available balance or up to the maximum participation levels allowed in a series of markets, or make several maximum bets on the same result for an event.

m) Users showing a winning profile with a specific player or team.

[12] SIGMA: the DGOJ's global betting market information service which manages alerts on suspicious or irregular betting.

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

n) Gambling strategies followed by previous users that had already been blocked being replicated in new users.

3.1.3. Risk scenarios in the analysis of bets made

o) Drastic changes in the betting pattern, such as bets significantly above the usual pattern, both in number and amount.

p) Evidence of Smurfing: customers where there are indications that they are managing several accounts at the same time to place their bet with lower amounts so as not to attract attention or maximise the return.

q) High activity of coordinated bets, with a difference of only seconds between them before the operator lowers the price or withdraws the event.

r) In combination bets, those that have more than one occurrence in an alerted event.

s) Very specific, individualised bets without a connection with previous gambling patterns, for example in tennis, bets on a specific game or set.

t) Unusual bets camouflaged within a multiple bet that includes low and very safe bets.

3.1.4. Actions to take in the described scenarios

An alert must generate the following actions:

- Communication of the alert to the DGOJ through the SIGMA service.
- Inform the police if there are suggestions of a crime.

3. Management of fraud risks

The specific risk management system must be adapted to the reality of each operator - type of gambling offered, marketing channels used, customer type, means of payment allowed or technology used. However, there are general principles that are transversal and their application is necessary for any type of operator. To properly implement a risk detection and management system, consultation and implementation of the following standards is recommended:

- UNE-ISO 19600: Compliance Management Systems. Guidelines.
- ISO 31000: Risk management.

The aforementioned standards define and explain the implementation of a compliance management model based on risks in the organisation in greater depth and establish general principles such as:

1. The gambling operator must implement a **Regulatory Compliance Management System** and Good Governance Principles (ISO 19600).

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

2. The gambling operator's organisation chart must include someone responsible for regulatory compliance ("**Compliance Officer**" or similar position), in charge of the company's internal and regulatory control. This position must have independence and report directly to senior management.
3. There must be **training programmes on fraud in gambling** for all internal staff. In this regard, special attention shall be given to staff making up the UHD (User Help Desk) or SAC (Customer Service), the personal managers of customer accounts and, in general, any service with a direct customer relationship.
4. The gambling operator must implement a **fraud in gambling risk management system** (ISO 31000). This management system is based on the definition, management and maintenance of a fraud in gambling risk matrix, defined according to the business model and idiosyncrasy of each operator.
5. The operator must implement **active monitoring procedures for its gamblers** that allow it to have a first data analysis of its gamblers and which becomes the starting point for further risk analysis. This process, also known as Know Your Customer (KYC), must be integral and provide feedback from the Due Diligence processes established by the operator in terms of anti-fraud regulations, money laundering and financing of terrorism, the prevention of sports events fixing, as well as processes that include interactions with gamblers such as the management of claims and incidents.
6. There must be a **communication channel with official bodies** within the operator with at least the following:
   - In the event of suspicions or indications of money laundering, operators are obliged to inform **SEPBLAC** (http://www.sepblac.es/).
   - In other types of fraud that could lead to crimes being committed, operators are obliged to notify the **Police**.
   - The information obligations with the **DGOJ**, such as the information in the Internal Control System of the user registration statuses, the quarterly report of blocked accounts and the immediate communication of alerts on bets within the SIGMA platform.

4. ANNEX – Bibliography

Certification standards:

- UNE-ISO 19600 Compliance Management Systems. Guidelines.
- ISO 31000- Risk management.

Documentation on the design of Compliance Management Systems:

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es

- The FATF's 40 recommendations create a basic framework for the fight against money laundering.
  http://www.sepblac.es/espanol/informes_y_publicaciones/40%20recomendaciones_feb2012.pdf

  http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

- Document on the approach to the prevention of money laundering and the financing of terrorism from a risk-based approach.

  http://www.sepblac.es/espanol/informes_y_publicaciones/documento%20_recomendaciones_sobre_medidas%20_control_interno_PBCFT.pdf

  http://www.sepblac.es/espanol/informes_y_publicaciones/38960576.pdf

C/ ATOCHA, 3 | TEL: +34 91 571 40 80
28071 MADRID | FAX: +34 91 571 17 36
dgoj.dgeneral@hacienda.gob.es