

Opinion

“What can the Internet do?”

bwin e.k.

**Rudolf-Breitscheid-Straße 20
02727 Neugersdorf**

Report No. 63002072-01-06

Köln, June 2009

TÜV Rheinland Secure iT GmbH

General information on the study

Client: bwin e.k.

Rudolf-Breitscheid-Straße 20
02727 Neugersdorf

Commissioned

Institute: TÜV Rheinland Secure iT GmbH

Unternehmensgruppe TÜV Rheinland Group

Competence Center IT Prozesse IT Security
51105 Köln

Tel. 0221 - 806 1615 / Fax 0221 - 806 1580

E-mail: secureit@de.tuv.com

Scope of the Study

Regulatory and self-commitment options in online gaming

Report No.: 63002072-01-06

Project Leader: Klaus M. Rodewig, Head of Engineering Business Division

Köln, 3 August 2009

Table of Contents

1	Summary	4
2	Introduction	6
2.1	Internet architecture	7
3	Online-Games and Online Betting	18
3.1	User registration	18
3.1.1	Master data verification	19
3.1.2	Abuse and data protection	20
3.1.3	Micro-deposit	21
3.2	Checking gaming and betting transactions	21
3.3	Financial transactions	22
3.4	Gaming fraud	26
3.5	Betting fraud	27
3.6	Money laundering	29
3.6.1	Mandatory customer registration	29
3.6.2	Identification.....	29
3.6.3	Risk assessment	29
3.6.4	Persons with a political profile.....	30
3.6.5	Notification duty.....	30
3.6.6	Appointment of designated money laundering reporting officers	30
3.6.7	Retention periods	30
3.6.8	Training.....	30
3.6.9	Monitoring and analysis of financial transactions	30
3.6.10	Know your customer (KYC)	31
3.6.11	Cooperation with financial institutions.....	31
3.6.12	Prohibition of cash transactions	31
4	Blacklist	32
5	Gaming Addiction	33
6	Bibliography	34

1 Summary

TÜV Rheinland Secure iT GmbH, a member of TÜV Rheinland Group, was commissioned by bwin e.k. (hereinafter “bwin”) to draw up an opinion on the possibility of anonymous online gaming on the Internet if relevant regulations and voluntary commitments are in place or whether anonymous gaming can be identified and prevented by implementing adequate technical measures.

In its opinion, TÜV Rheinland Secure iT GmbH examines the following questions:

- How does Internet gaming work?
- What methods of authentication and identification are available on the Internet?
- What possibilities are there to verify that a customer is of age?
- How to identify conspicuous customer behaviour (fraud, problem gambling) on the Internet?

In addition to the above questions, the opinion examines the risks and opportunities offered by the Internet as an online gaming distribution channel, focusing on online bets (sports betting, society betting), card games (poker, etc.) as well as on skill and casino games. Online role-playing games and computer games offered in casinos were expressly excluded from this opinion.

1. How can the gaming behaviour of an online gamer be monitored?

As inherent feature of the system, all the activities of an online player are recorded. Such data can therefore be reviewed for anomalies by using appropriate methods. In their own interest, i.e. to prevent fraud or abuse, various providers have established comprehensive methods of analysis to detect anomalies and exclude the players concerned from their gaming operations.

In contrast to conventional casinos, where it is impossible to track all gaming activities, online gaming provides an ideal opportunity to monitor the gaming behaviour of players. By comparing this behaviour with the gaming behaviour of an entire community and with the gaming behaviour of a single player, accurate findings regarding potential problems such as fraud, money laundering, or gaming addiction, can be derived.

Gaming addiction research provides indications on how problematic gaming behaviour is expressed. Certain behavioural patterns such as chasing losses may indicate problematic gaming behaviour. With online games, gaming behaviour is recorded completely, which allows a thorough check for irregular gaming behaviour and an opportunity to respond appropriately.

2. Is anonymous online gaming possible?

Players can register by providing false details in order to participate in games or bets. Money can also be deposited anonymously to gamble and bet. By using information service providers to identify customers, online gaming and betting providers however are able to verify in real-time whether the details provided by a customer are accurate or coherent. In this way, false information can be identified promptly and the relevant gaming accounts can be blocked. Furthermore, players cannot

have any of their winnings from gaming or betting activities paid out without previously providing proof of their identity. A player is required to disclose his/her identity upon a payout at the latest. As it is impossible to have winnings paid out when gaming anonymously, there is no incentive for players to hide their identity.

3. How can we verify and ensure that an online player is of age?

In the identification process of players, a player's age as well as any other master data can be reliably determined through adequate logic and cross-checks and by using the databases of external service providers (Section 3.1.1). ID verification providers such as GB Group offer identity and age verification services, which can be used in real-time on the Internet, thus ensuring the protection of minors when providing such services.

4. Is it possible and expedient to set up a blacklist for all providers?

To verify the identity of players and betting customers it is necessary to use external information sources and databases (Section 3.1.1). These databases contain sufficient information to clearly identify people. It is deemed to make sense to set up a separate blacklist for online gaming and betting; much rather, it would be preferable to provide feedback to the operators of said databases to allow for the (industry-wide as well as intersectoral) identification – taking into account the provision of privacy law – of conspicuous players and customers.

2 Introduction

TÜV Rheinland Secure iT GmbH, a member of TÜV Rheinland Group, was commissioned by bwin e.k. (hereinafter "bwin") to draw up an opinion on the possibility of anonymous online gaming on the Internet if relevant regulations and voluntary commitments are in place or whether anonymous gaming can be identified and prevented by implementing adequate technical measures.

In our opinion we examine the following questions:

- How can the gaming behaviour of an online gamer be monitored?
- Is it possible and expedient to set up a blacklist for all providers?
- Is anonymous online gaming possible?
- How can we verify and ensure that an online player is of age?

An online game is a computer program that has been designed in such a way that a player is able to access and use the program only on the Internet. The gaming provider operates a server infrastructure accessible via the Internet and players can access this server via the Internet to play online games. The contents of an online game may be of any nature whatsoever and may be provided as any game. In addition to online-gambling, this opinion also investigates sports bets, which are designed as online services and hence can only be accessed and used by customers via an Internet connection.

The Internet in its current form resulted from a US Defence Ministry research project undertaken in the 1960s. During the 1990s, the system which had originally been exclusively for military and academic purposes developed into a system used chiefly for commercial purposes by companies and private users. Today, it would be impossible to imagine everyday life without the Internet. Offers such as online-banking, e-commerce in all of its forms, e-mail, chat, and recreational activities such as online gaming are used by the majority of the population.

In terms of the Internet's commercial use, two issues are of particular relevance: anonymity and data protection. Providers of Internet-based commercial services have a vital interest in knowing who customers are. Although Internet technology makes it technically possible to use the Internet anonymously, the exact identify of users can be determined when they use services – at non-technical level – and anonymity with the intention of abuse can be prevented.

Data protection on the Internet needs to be studied at two points: the path taken by data through the Internet and the respective system operator. It is possible to ensure the safety of data during transmission on the Internet through adequate and well-established encryption methods such as

SSL/TLS¹. The protection of data held by system operators, e.g. by commercial service providers on the Internet, can also be ensured through a wide variety of appropriate methods.

2.1 Internet architecture

A prerequisite for using online games or online betting services is an Internet connection between the gaming provider and the player. Such an Internet connection is no direct connection between the player and the provider, i.e. unlike a phone connection. Rather, both the player and the provider are connected to the Internet through separate and unrelated connections, with the Internet acting as a switch and carrier between these two connections without the player and/or provider being able to influence the type and path of the connection on the Internet (figure 1).

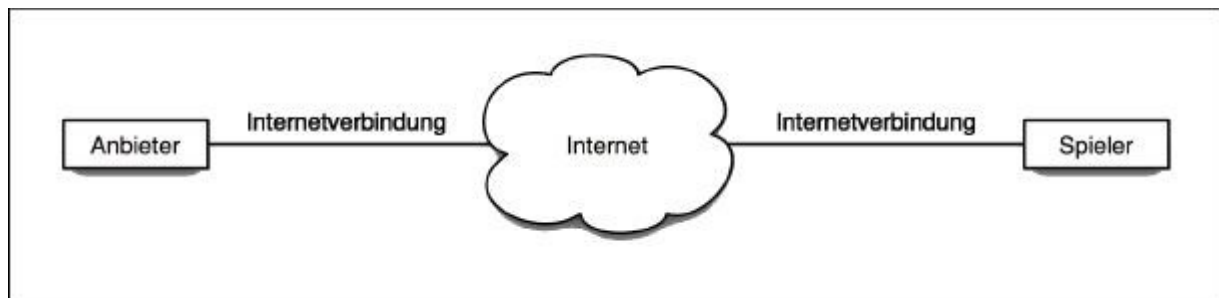


Figure 1: Structure of an Internet connection.

While the provider is usually connected with the Internet via a land-based connection or uses special service providers to operate its server infrastructure via a direct Internet connection, the player has a number of options to choose from when connecting to the Internet. Established types of Internet access for end users and private consumers include the digital subscriber line (DSL), analogue modem connections, ISDN dial-up, mobile telephony, or connections using WLAN hotspots. WLAN hotspots provide Internet access with the customer either accessing the Internet either – in case of publicly accessible hotspots – free of charge and anonymously or against payment and/or identification – in case of closed hotspots. Additional Internet access options for players include corporate networks, where a player uses his/her employer's infrastructure, for instance, to use Internet services.

The Internet is a decentralized aggregation of independent networks and computer systems. With the exception of country-specific regulations, there is no joint management or regulation of operation and of the data transported using such networks. There is in particular no centralized management and control body in charge of the Internet.

All networks that have been combined to create the Internet have one thing in common, i.e. the use of the TCP/IP protocol suite for communication. This protocol suit comprises various network protocols, which are used to run Internet communications. The protocol suite was developed and

¹ <http://tools.ietf.org/html/rfc2246>

implemented with the objective to avoid breakdowns in network areas leading to a collapse of the entire communication.

For this reason, the implementation of TCP/IP is package-based. This means that the data streams that need to be transmitted from sender to receiver are divided into data packages by the sender. These packages are then transmitted independently from one another. The receiver puts the data packages back together into one coherent data stream. The network's system stability is ensured by allowing for data packages to arrive at the receiver along various paths between sender and receiver. These paths are not determined in advance. If one path fails, then the data packages are transmitted using an alternative path.

Figure 2 depicts parts of the diagrammatic structure of the Internet. The shown networks symbolise the various networks of which the Internet as a whole consists of. Both direct and indirect connections exist between the networks. The communication between two end points, e.g. online player and provider, does not require a direct connection between the two communication partners. Data can be transmitted along any paths.

Among other possibilities, the following connecting paths between player and provider are possible in figure 1:

Player ->> network 1 ->> network 2 ->> network 6 ->> network 9 ->> provider

Player ->> network 1 ->> network 5 ->> network 6 ->> network 9 ->> provider

Player ->> network 1 ->> network 4 ->> network 9 ->> provider

Depending on the availability of paths and factors well as on the available bandwidth and utilisation, Internet paths are selected dynamically with the aid of so-called routing protocols.

Routers are positioned as switches between the individual networks and independently search for the best path for a data package. Routers are switching computers that transfer data packages between the networks. Knowledge of the connected networks available and the selection of routes are recorded in routing protocols, which routers use to communicate with each other and to exchange information about these very same parameters. Because of this dynamic communication and the resulting dynamic path selection it is impossible to predict the path of a data package on the Internet.

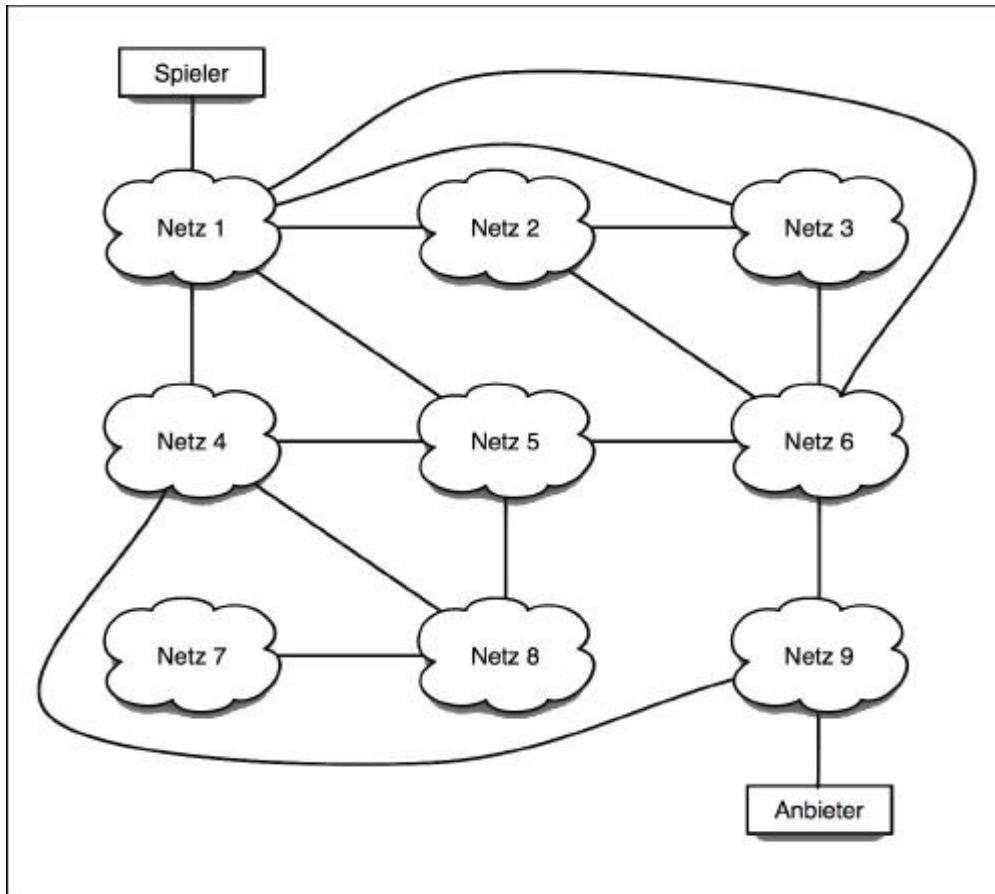


Figure 2: Structure of the Internet.

Figure 3 depicts the route from an access point into the Vodafone UMTS network to the server www.tuvdotcom.com. The figure shows that data packages pass through four different networks, which are operated by four companies that are independent of one another. Transfer points between the networks may be dedicated network gateways or central Internet nodes², in which a number of networks converge and are connected through routers.

² <https://www.euro-ix.net/member/m/isp/choosing/ixplist>

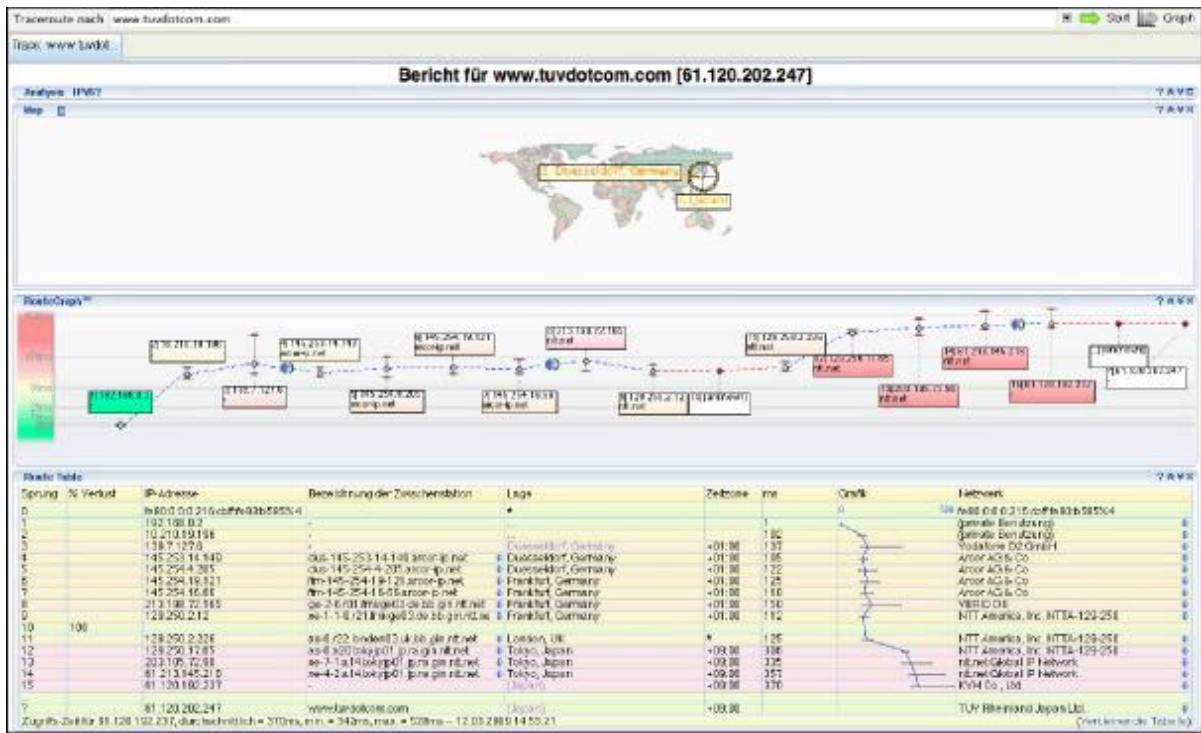


Figure 3: Route UMTS dial up for www.tuvtocm.com.

To understand Internet technology it is necessary to describe not only the structure of the Internet and the network's ability to select paths dynamically, but also the TCP/IP protocol suite, which is represented by the TCP/IP reference model (Tanenbaum, pp. 35 et seq.). The OSI reference model is often used erroneously with descriptions of Internet technology. This model however, is of no relevance in respect of the TCP/IP reference model and merely constitutes an abstract model of the structure of networks.

The TCP/IP reference model (cf. figure 4) defines five layers through which network communications run. From the lowest to the highest level, data from the respective higher layer are packaged into the data packages of the respective lower layer.

The network access layer is located at the lowest level and consists of the physical connection and a protocol to connect hosts within the local network. The protocols of this layer are not part of the TCP/IP protocol suite. Possible protocols of this layer are, especially with private users, the Ethernet (local network), IEEE 802.11 (WLAN) and PPP (modem or mobile phone connections).

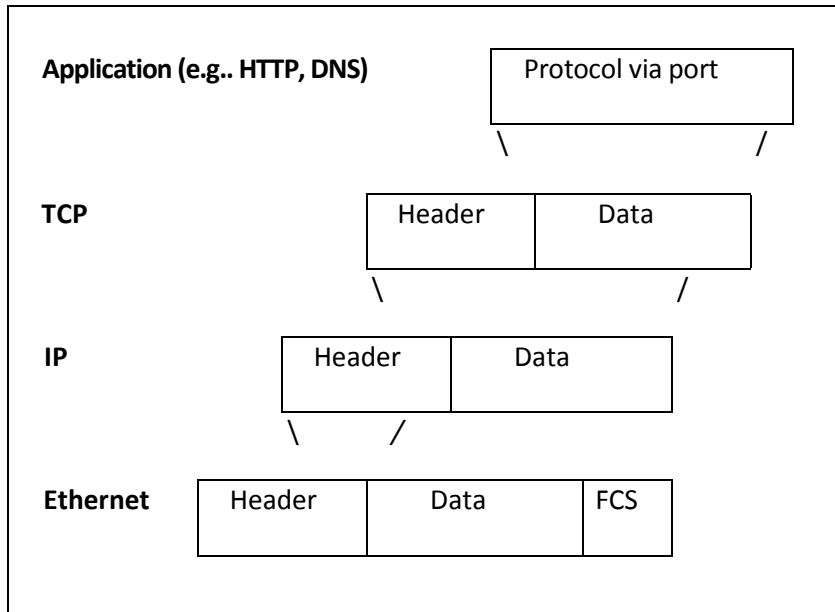


Figure 4: TCP/IP reference model on Ethernet basis.

The TCP/IP protocol suite commences at the third layer, the Internet layer, which is represented by the IP protocol ("Internet protocol"). The tasks of this layer are to transport data from the higher layers and select paths beyond the local network. In so doing, the IP provides the option of routing, which allows the paths along which data packages are sent on the Internet to be defined.

IP packages the data of the higher layers in data packages and sends them independently of one another. In so doing, it is not the task of the Internet layer to take note of the sequential order of the sender's packages. Depending on the respective path selected, and thus due to delays in transmission, they may indeed arrive at the receiver's in an order that differs from the one intended by the sender. It is the task of the next-higher layer, the transportation layer, to determine the correct sequence and thus to ensure the accuracy of the transmitted data.

The transportation layer is represented in the TCP/IP reference model through the two protocols TCP (transmission control protocol) and UDP (user datagram protocol). TCP is a connection-oriented protocol that establishes a reliable connection between sender and receiver and ensures the integrity of the transferred data. In so doing, it checks the transferred packages at the receiver's end and reconstitutes the correct sequence after transmission. If packages are missing or in cases of transmission errors, it is the task of the transportation layer to request renewed transmission of the relevant packages from the sender.

UDP is a connectionless protocol, by which the sender sends UDP packages to the receiver without establishing a connection to the sender. As it is impossible to check the transmission of these packages in the absence of a controllable connection, UDP is used only for special services. Therefore, only TCP is of interest for applications such as online games or online betting.

The transportation layer introduces the so-called ports, virtual connections at a host that include specific services. For example, a web server is usually available at port 80. Coded communication with the web server usually uses port 443.

In the TCP/IP reference model, the application layer is located above the transportation layer. The transportation layer packages the data of the application from which the data to be transferred originates from. In the case of a web server, the protocol of the application layer is the hypertext transfer protocol (HTTP). All functionalities of an application, such as session management, coding etc. will be shown in this layer by the relevant protocol. Other routine protocols of the application layer are POP3 (e-mail receipt), SMTP (e-mail dispatch), DNS (domain name system) and SSH (secure shell).

The process of name resolution on the Internet is of relevance in connection with online services such as online games and betting services. All communication partners on the Internet have a unique identification on the Internet layer, i.e. the IP address, which identifies them as a distinct member of a network connected with the Internet. Communication partners on the Internet are exclusively addressed through their IP address. In the currently prevailing IP-Version 4, the IP address is a 32-digit binary.

To make addressing easier for Internet users, what is known as the domain name system was implemented. It is now possible to assign names to IP addresses so that users of an online service only need to memorize a name instead of an IP address. These names are referred to as fully qualified domain names (FQDN).



Figure 5: Google homepage using IP address.

Figure 5 shows the Google homepage, which has been prompted by entering the IP address of the Google server (209.85.135.104) in the browser's address bar. By contrast, in Figure 6, the homepage

has been prompted via the DNS entry www.google.de, which in DNS has been assigned the IP address 209.85.135.104.



Figure 6: Google homepage using DNS.

Figure 7 shows the sequence of a DNS query after a user has entered the address www.google.de in the address bar of his/her browser (step 1). In step 2, the user's operating system asks the competent DNS server (Rodewig, pp. 115 et seq.) to provide the IP address for the name www.google.de. The DNS server returns this address in step 3, enabling the user in step 4 to address the server www.google.de by using its IP address. Name resolution on the Internet merely serves the purpose of facilitating its use and is not a technical necessity for communication between computer systems.

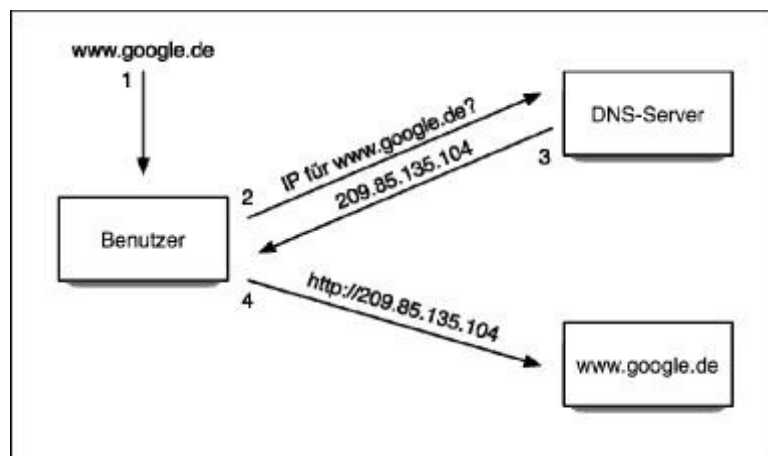


Figure 7: DNS query for an http request.

The DNS namespace on the Internet is structured hierarchically. Large areas are divided into top-level domains, e.g. top-level domains for individual countries. The top-level domain in the DNS

hierarchy is followed by the domain, which might be assigned to a company, a person or to an organisation. A domain may be divided into sub-domains, ultimately followed by a host name – the name of a specific system. The components of a DNS name are comprised in the hierarchy in descending order from right to left.

In the previous example of the DNS address www.google.de the suffix “de” is the top-level domain for the namespace assigned to the Federal Republic of Germany. Top-level domains for countries are usually identical with their international country codes. The name component “google” in the DNS name shows the domain “google.de”, a domain registered for Google below the top-level domain “de”. The leading identifier “www” in the DNS name stands for the system with the name “www” within the domain “google.de”. This allows for addressing precisely this system by calling up the DNS name www.google.de.

The registrar of the respective top-level domain has administration rights over a top-level domain. In Germany this is DENIC eG³ for top-level domain “de”. The owner of the respective domain has administration rights to that domain, i.e. in the case of www.google.de that would be Google.

The domain name system provides two different types of DNS servers to reply to DNS queries. The first type is that of authoritative DNS servers. These are DNS servers responsible for the administration of a specific domain which reply to queries regarding that domain using their own database, the so-called zone. For each domain only a limited number of authoritative DNS servers is available.

To be able to guarantee DNS server replies throughout the entire Internet at an acceptable speed, non-authoritative DNS servers are used in addition to the limited number of authoritative DNS servers. Non-authoritative DNS servers are frequently located in the access networks of Internet providers and are used as DNS servers by the respective users. Non-authoritative servers do not maintain any original databases, but upon receiving a DNS query from a user in a chain of hierarchies query other DNS servers up to the authoritative server of the relevant domain. The non-authoritative DNS servers buffer the result of this query, enabling them to supply the answer from their buffer in case of a repeat query, when the non-authoritative DNS server has to contact the authoritative DNS server again only if the period of time defined by the authoritative DNS server for this domain has expired.

³ <http://www.denic.de/>

3 Online Games and Online Betting

When using online games and online betting, a distinction must be made between registration, gaming as such as well as actions and sequences after a game or a bet has been completed.

When looking at online gaming and betting services, two terms must be separated with regard to the users of such services. The first term is that of the player or user – both terms are used synonymously here. The user represents a natural person, i.e. a customer of an online gaming or betting provider. The second term is that of a user account. A requirement for using the online service is the establishment of a personal user account with the provider.

A player who wishes to use a gaming or betting service on the Internet usually has no interest in providing false personal details when setting up a user account. Verification of the information provided by the player and thus of the player's identity by the provider on the other hand is necessary where abuse or fraud is possible. This is the case with offers provided by minors, suspected money laundering, betting fraud, gambling addiction or other anomalies, for instance.

3.1 User registration

Customers are identified before a game or bet by way of a registration process, where a customer account is set up with the customer's master data and the customer selects a user name and password, which he/she can use for identification and authentication to participate in online games and/or bets. As usually only one user account is permitted per player, it is possible to allocate all gaming and betting-related transactions to one customer. Typical information a customer must provide during the registration process includes:

- name/ given name
- residential address (incl. country)
- date of birth
- phone number
- e-mail address

The e-mail address is of central significance for online gaming and betting, since business partners usually communicate exclusively by e-mail on the Internet. However, e-mail is not a unique characteristic, since e-mail addresses – as described in Sec. 3.1.1 – are not tamper-proof.

Another safety criterion frequently used in online gaming and betting in addition to a password is a so-called security question. The user deposits a question, which only he/she can answer. This enables the user to identify him-/herself vis-à-vis the provider if he/she forgets his/her password.

3.1.1 Master data verification

A player may enter any data to register as a user of an online service. Easy to implement verification options in the framework of the respective regulations under data protection law, e.g. street name, place, post code or phone number match, can be carried out directly when the data is entered. Further and comprehensive verification options are offered by companies specialising in identity verification such as GB Group⁴ in Great Britain or also 192.com. In adhering to the KYC principle ("Know your customer"), these providers consolidate data about persons from various sources into one database. Cross-checks and logic checks allow for the very accurate verification of the identity of persons.

The first possible and most fundamental check is the accuracy of the address entered by the player (street name, place, post code). If this data does not match, i.e. if the entered street name does not exist in the entered city or town, this is false or at least faulty information. Once the address has been verified, the relevant service provider can carry out further checks. Databases such as those offered by GB Group make it possible to verify whether a person does indeed live at the entered address or not. This can be done with a high degree of likelihood, since the database of GB Group – which is given only as an example here – like the databases of companies such as Creditreform⁵, Schufa⁶ or Bürger⁷, is fed from a variety of independent sources, which allow for mutual comparison and alignment and thus for a high hit rate. Data sources that are included in such databases for checks include sources with data regarding bank accounts, credit cards, date of birth, violations of law, business relationships, loans etc. In some cases this allows not only for verifying whether a person does indeed live at the entered address, but also if the entered bank account or credit card is his/hers and if it is registered at the entered address, if the age given is accurate or if anything special is known about this person.

Electronic real-time data processing in case of online games and bets allows for the above check to be carried out immediately after the data have been entered by a player. It is thus possible to identify incorrect data before a player is able to use services without authorization or to perpetrate fraudulent actions. Periodic checks of the data of already registered players may unearth irregularities or anomalies that have arisen subsequently and thus a comprehensive and effective control of all players.

If a player is intent on entering false details, he/she may do so, but the data will be identified as false by way of a downstream check. To verify the e-mail address entered by the player during registration, many providers immediately after registration send an e-mail to the registered e-mail, including a hyperlink that needs to be activated by the player. In this way, it is possible to verify at least that the e-mail address is genuine.

⁴ <http://www.gb.co.uk>

⁵ <http://www.creditreform.de/>

⁶ <http://www.schufa.de/>

⁷ <http://www.buergel.de/>

In doing so it has to be noted that an e-mail address is not a reliable criterion for identification. With providers offering free e-mail services such as GMX, Yahoo, Google, Hotmail, etc., it is possible to set up e-mail accounts by entering false details, i.e. a player who does not wish to disclose his/her identity can open an e-mail account using false details, which he/she could then use to set up a user account, again with false data. As the used e-mail address is fully functional in such a case, the validity of the e-mail address will be verified successfully. If a user uses an anonymisation service such as JAP for all of his/her transactions on the Internet, then it is also not possible for the e-mail and gaming provider to determine his/her identity via the IP connection.

3.1.2 Abuse and data protection

The combination of user name, password, and security question represents verification exclusively by way of knowledge. This type of authentication can be abused by third parties, e.g. by guessing the registration parameters or by spying them out. One way of safeguarding registration data is to extend the factor 'knowledge' by the factor 'possession'. This can be ensured in the form of tokens, mobile phones, or so-called unique hardware devices (UHD). One frequently used example for transactions based on knowledge and possession is online banking with SMS messaging of TAN codes. In this case, the user needs his/her registration data which consists of user name and password to log in to online banking. Once the user wishes to carry out a transaction the bank sends an SMS with a valid TAN for the transaction to the user's mobile phone. This ensures that only someone who knows the valid log-in data and who is also in the possession of the mobile phone defined for TAN messages is authorised to carry out transactions.

UHDS are available in various forms. In all cases, the issue of security must be balanced out with that of ease of use. A UHD that is linked to a specific computer would prevent a player from playing or placing bets on the Internet by using other devices as well. UHD in the form of tokens, such as the RSA SecurID-Token⁸ are portable, can be used anywhere and prevent the abuse of players' accounts by unauthorised persons who have gotten hold of their log-in data. On the other hand, tokens and UHDS do not help in the identification of players.

3.1.3 Micro-deposit

One option to verify the accuracy of a bank account provided by a player are so-called micro-deposits: The provider transfers a small amount to the player's nominated bank account together with a unique identifier as reference, which the player is required to enter as to activate his/her online account. This makes it possible to verify that the relevant player has access to the account statement of that bank account.

⁸ <http://www.rsa.com/node.aspx?id=1156>

3.2 Checking gaming and betting transactions

Conspicuous behaviour such as unusually high stakes or unusually high deposits can be detected automatically and can be thoroughly analysed in a downstream process. The clear allocation of deposits to players' accounts makes it very easy to verify how much money a player has deposited and how much he/she has been paid out. Departures from average values can be detected right away. In connection with gaming addiction it is also possible to detect conspicuously frequent or prolonged gaming and to block the relevant gaming accounts. In order to detect and to prevent betting fraud, it is possible to check the course of bets and games automatically for any conspicuous patterns and thus enable the provider to intervene. The simple analysis of playing time too is an important reference to the gaming addiction risk of a player.

These points are in contrast to the control and intervention options a real casino or betting shop has, where such control options do not exist given that they involve no electronic data processes and no or only rudimentary data in connection with transactions can be assigned to individual visitors.

From initial registration it is possible to record and store (log) every single activity of a customer during all subsequent log-ins. In this way, it is possible to keep record not only on the preferences, such as language, but also favourite types of games (e.g. sports betting) or types of sports (e.g. football, mainly Germany). In addition, any changes to the user details - if permitted at all - are stored. For instance, it is not permitted to change the name at a later stage, unless official documents can be provided showing that the name has changed, e.g. by marriage.

Over time, customer profiles are created in this way, permitting statements to be made on the gambling behaviour of individual customers. Recording such gaming activities does not only allow conclusions regarding customer behaviour to be drawn, but also supports providers in recording conspicuous gambling behaviour that deviates from the norm and to initiate relevant verification processes. Deviating gaming behaviour may have a variety of causes. On the one hand, problem gaming might be expressed through prolonged and more intensive gaming activities for instance. On the other hand, it is possible to detect betting fraud by way of conspicuously high stakes on predestined types of sports or money laundering by way of unusual transactions.

The logged data include:

- time of log-in and log-out (period in-between is the gaming period)
- time and type of bets placed
- time and type and hands played in case of poker or other virtual card games
- times and course of other virtual games
- selected language

Thanks to this logged data it is possible in case of disputes, for example, to then clearly trace which player has played which hand first or when a player has placed a bet (e.g. five minutes before the decisive goal was shot or five days before the match).

3.3 Financial transactions

Financial transactions are necessary when using online games and online bets so as to be able to transfer stakes and winnings between player and provider. Deposits can be paid by the player to the provider in various ways. Well-established procedures include the use of credit cards, direct debits, transfers, Paypal⁹, Click&Buy¹⁰, etc.

All these procedures have in common that a person can use them only after he/she has been identified by the respective payment provider. It is legally impossible to obtain a credit card or bank account by using a false identity. Therefore, the provision of payment options when setting up a user account for online games or online bets involves information that can be verified by the provider and can be directly connected with other information provided by the player (name, address, etc.) and thus allows for direct verification of the data. Even if the information provided in addition to the payment details is inaccurate, the provider is able to identify the player by checking the payment details.

Apart from the enhanced security that providers require to be able to correlate payment and addressing data by way of geo-localisation, providers are furthermore able to use such information to notify customers about possible cases of identity theft. The majority of those affected by identity theft realise this fact only with considerable delay. If a provider in the course of a security check finds that a customer might have become the victim of identity theft, e.g. through the unauthorised use of payment means, then the provider may both block the defrauder's user account and also notify the customer. This approach provides considerable additional value for customers and may encourage them to provide all their details truthfully in order to receive the greatest possible degree of security and benefit from the respective provider's early warning options.

In addition to the personalised payment options there are others that allow for depositing amounts without checking the identity. One example is the Paysafecard¹¹. In this procedure, a person buys a PIN code from a sales outlet and this code can be used to activate non-personal credit on the Internet. If cash is used, the purchase can be completed anonymously. PIN codes can be purchased in drug stores, petrol stations, or supermarkets for example. With the aid of this payment option, a player is able to anonymously deposit money into a gaming or betting account.

The potential chances of winning are an essential feature of online games and online betting. The disbursement of winnings from online games and online bets is possible only by providing a valid bank account and – depending on the provider – after separate verification of the player's identity, e.g. by sending in a copy of the player's ID card. So even if a player does not register with accurate data and anonymously deposits money by using a procedure such as Paysafecard, he/she has to disclose his/her real identity for the payout of winnings – hence, while it is possible to play

⁹ <https://www.paypal.com>

¹⁰ <http://clickandbuy.com>

¹¹ <http://www.paysafecard.com>

anonymously, this will in no case lead to financial winnings, thus making it unattractive for gaming addicts and players with the intention to defraud.

As regards the risk of identity fraud, it needs to be noted that in the context of anti-money laundering measures providers permit deposits and payouts only in and from accounts and credit cards based in the same country where the player is located. A German player, for example, can use only German bank accounts or German credit cards. In general, providers of online games and online bets are subject to "Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing". To comply with this Directive, providers are required to implement comprehensive measures so as to detect and prevent any anomalies in financial transactions and, as the case may be, to pass the information on to the law enforcement agencies.

This includes regular comparison and alignment with terrorism data bases (e.g. UrU¹² of GB Group) and monitoring of unusual activities and transactions that deviate from the normal gambling behaviour of the respective player, for instance. Such activities deviating from the norm include unusually high deposits and stakes, deposits which are sought to be paid out again without having played or placed bets and a change in the means of deposit and disbursement for example. What is more, activities violating the Terms and Conditions including the use of several accounts by a player or the use of one account by several players are also conspicuous.

Activities that deviate from the normal paying behaviour of an individual player include a sudden increase in the stakes compared to the stakes in the player's previous gaming or a sudden change of games or bets with an associated change in the stakes.

Both games and bets as such as well as the processing of all master and movement data in case of online services are done electronically due to nature of the system and therefore allow for immediate processing with regard to anomalies. Online gaming and betting providers are therefore in a position to automatically and efficiently check their customers' gaming behaviour based on the data collected in games and bets and in this way to identify conspicuous players. Adequate cross tests and logic tests of master data allow for the identification of false information and conclusions can be drawn on individual players by conducting random checks of gaming and betting behaviour.

In connection with the fact that a player has to disclose his/her identity at the very latest when wishing to receive a payout, the likelihood of anonymous online gaming or betting must be regarded as non-existing, in particular compared to conventional gaming venues such as arcades or casinos, where neither the identity nor the bank account of a player are required for deposits or withdrawals. Statutory provisions such as those regarding the protection of minors can be implemented effectively by way of the identity verification as required when paying out winnings. Recognising conspicuous players through the automated analysis of gaming data is simple too and has already been implemented successfully by various providers.

¹² <http://www.uru.co.uk/>

Cash transactions are usually impossible in case of online games and bets, since there are no physical encounters between player and provider that would allow for cash transactions.

In online gaming, all financial transactions are checked continuously for certain parameters so as to be able to detect irregularities or deviations. In doing so, the following parameters are checked by many providers when the first deposit is made:

- initial deposits that exceed a defined limit
- unusually high deposits
- deposits that are not immediately used for gaming
- deposits that are immediately followed by payout requests without any games played in the meantime
- consistency of the country of registration with the country of the credit card of bank account
- Are any of the parameters included in a blacklist?
- Is the same credit card or the same bank account used by several customers?
- Is one customer using several credit cards or bank accounts?

If one or several of the specified parameters apply, the provider can perform additional checks and in case of justified suspicions temporarily close the gaming account. Depending on the payment method selected by the customer, further identity controls may be performed or classifications may be applied for the sake of risk management in accordance with the anonymity of the means of payment.

In case of deposits made by credit cards or bank accounts, for example, the credit card or bank account holder's details are compared with those provided by the customer upon registration. Additional identification of the customer (e.g. sending-in copies of ID cards), also known as enhanced customer due diligence, may be initiated in case of relevant suspicious facts.

If the customer has not yet been identified in the registration process by way of identification verification providers, national databases, the transmission of ID papers or a bank account, this must be done in the lead-up to the first payout at the latest. To ensure the accuracy of the information provided by the customer upon registration, the provider can choose from a range of verification methods. As part of a payout, the customer's activities are again checked for specific conspicuous parameters.

These include:

- payout requests were made immediately after a deposit has been made without having played in the meantime (suspected money laundering)
- high payouts
- withdrawals to accounts or credit cards with the country of the account or credit card not being identical with the country of the customer's registration

- transaction details (e.g. credit card number) are included in a blacklist
- the same credit card or the same bank account is used by several customers
- several credit cards or bank accounts are used by one customer
- little or no stakes since the deposit
- use of other means of deposit since the last payout
- use of other means of payout since the last deposit

3.4 Gaming fraud

The absence of the customer's physical presence makes it possible for customers to simultaneously act on several platforms or to even participate in one and the same game offered by a provider. Also, several customers can share one gaming account.

Especially in case of tournament games/P2P games such as poker, collusions are possible, constituting a special case of game manipulation, where two or more players agree to participate in a specific poker game, meet at the virtual poker table, pretend to be opponents like all of the other players, but illicitly come to an arrangement and share the winnings. Or: One and the same player opens two gaming accounts and in this way participates twice in a game, thus increasing his/her chances of winning.

The data and processes recorded in online gaming make it relatively simple to uncover this phenomenon termed collusion. Collusion is suspected in the following cases:

- two or more customers always sit down at the same virtual poker table,
- two or more customers have the same account or credit card data,
- two or more customers have similar user names, similar passwords, similar addresses etc.

Characteristics of a customer with several gaming accounts or of collaborating customers are:

- similar customer details
- similar user names and passwords
- same country of registration
- same language
- same or similar e-mail addresses
- same payment methods
- identical bank account, credit card details, etc.
- same log-in times
- same gaming interests

To prevent collusion, online gaming providers have several options available.

- prohibition of opening more than one gaming account per customer (checking similar addresses, similar passwords, etc.)
- verification of this rule through the data provided at the time of registration by using ID verification providers, databases or comparison with ID papers
- further verification by way of comparing the payment method (same bank account, same credit card data, etc.)
- comparison of gaming behaviour (e.g. French customer who since registration has only placed sports bets on basketball in France and mainly on weekends, suddenly has started to play casino games during the week and no longer places any more sports bets – there is reason to suspect that the customer voluntarily or involuntarily has allowed a third party to use his/her gaming account)
- protection against the voluntary disclosure of data to third party or the theft of data by using a combination of user name, password, personal question and a third verification stage, such as e.g. unique hardware device

3.5 Betting fraud

One problem with sports bets is the possibility of manipulating bets, i.e. betting fraud, meaning collusion between an athlete and sports club on the one hand and a bettor on the other hand who places high stakes on the – already known – result of a game or tournament with the intention of generating high winnings. Betting fraud is not a specific characteristic of online betting, but – as is known from relevant reports (cf. below) – is also known and constitutes a problem in the traditional betting business. In case of online bets, ongoing and detailed monitoring of all transaction parameters and gaming behaviour however, allows for the early detection of betting fraud. Specific parameters are thoroughly checked, since they are known to be prone to betting fraud:

- fringe sports
- sports where it is possible for a single athlete to influence the outcome
- venues, which are mainly located in susceptible countries
- bets on events that are relatively easy to manipulate

Deviating gambling behaviour too may be an indication of manipulation or insider knowledge:

- a customer places a bet on a sports on which he/she does not usually bet
- a customer places a bet on a sporting event at a venue that is different from the customer's usual betting habits
- a customer bets unusual high amounts for his/her standards
- a customer is trying to carry out transactions from a country other than that of his/her

registration

- a customer is using a deposit method that is different from his/her usual method of deposit.

So in case of one or several irregularities the provider might subject a bet to more scrutiny. By integrating providers in an independent organisation it is possible to detect and prevent betting fraud on the Internet early and more effectively than it is possible in the anonymous stationary betting business, which cannot be traced without any gaps. One example is the Hoyzer incident, where only the German betting provider Oddset suffered damage, whereas the various online providers were unattractive to the manipulators, as it was not possible to place anonymous bets.

By combining several online betting providers in transnational associations, such as the FIFA Early Warning System¹³ or the European Sports Security Association¹⁴, it is possible to use early warning systems in a first step to determine anomalies in certain sporting events and to pass that information on to other online gaming providers. If other online betting providers too have noted anomalies an alert is sent immediately to the event's organisers to enable them to check whether irregularities can be identified by athletes or clubs. In justified cases online betting providers furthermore agree to cooperate with the investigating authorities.

3.6 Money laundering

Generally, providers of online games and online bets are subject to "Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing". To comply with this Directive, providers are required to implement comprehensive measures so as to detect and prevent any anomalies in financial transactions and, as the case may be, to pass the information on to the law enforcement agencies.

In addition, the Financial Action Task Force (FATF) has issued recommendations for stationary gaming and for gaming on the Internet. The following measures are part of the EU's Anti-Money Laundering Directive implemented in the Member States and the recommendations issued by the FATF, which providers licensed in EU Member States are required to submit to:

3.6.1 Mandatory customer registration

As explained in Sec. 3.1, to be able to participate in real money games, customers are required to first of all register with the provider, providing name, address, and date of birth.

¹³ www.fifa-ews.com

¹⁴ www.eu-ssa.org

3.6.2 Identification

Implementation of the Directive furthermore requires that customers be identified prior to the first payout at the latest. If conspicuous gaming behaviour is suspected (high stakes, rapid succession of games), identification is required at an earlier stage. The rationale behind this is on the one hand to find out who the customer is, whether he/she is of legal age and on the other hand to allow providers to support criminal prosecution in respect of money laundering. If it is not possible to identify a customer, the provider is required to block the account for the time being.

3.6.3 Risk assessment

The handling of verification methods must be based on risk assessment. Customers who have been placed in higher risk categories must be subjected to more thorough checks, whereas customers in lower risk categories may be subject to reduced or simplified measures.

3.6.4 Persons with a political profile

Business relationships and politically exposed persons require the approval of their senior management or money laundering reporting officer. They are identified by using globally accessible public databases (e.g. WorldCheck).

3.6.5 Notification duty

Staff members who classify certain transactions as suspected money laundering are required to report this. In a second step, the provider is required by law to notify the competent authorities and the licensing authorities about suspected money laundering. Employment contracts provide for disciplinary measures in case of violations of the confidentiality principle, in particular in cases of money laundering.

3.6.6 Appointment of designated money laundering reporting officers

Providers are required to employ designated money laundering reporting officers within their company who are responsible for implementation of and compliance with the Directives.

3.6.7 Retention periods

According to the money laundering provisions providers are required to retain all transactional records for a period of at least five years after completion of a transaction and for five years after termination of a customer relationship for potential investigations by the competent authorities.

3.6.8 Training

The provider is required to train the relevant staff on a continuous basis (internally, but also externally, e.g. through the International Compliance Association, Mastercard Academy) to enable them to detect conspicuous behaviour and to handle potentially criminal transactions at an early stage.

3.6.9 Monitoring and analysis of financial transactions

To prevent money laundering, providers are required to monitor their customers' financial transactions and to check them with regard to deviations and anomalies.

3.6.10 Know your customer (KYC)

Starting from registration, providers are required to subject all customers to the KYC principle.

3.6.11 Cooperation with financial institutions

Providers agree in connection with money laundering to cooperate with financial institutions as well as with the competent authorities.

3.6.12 Prohibition of cash transactions

Even apparent cash transactions, such as transactions made through Western Union perform an at-point identification of sender and recipient. The recipient is required to provide official identification documents whenever he/she is (personally) receiving the money.

Further measures to prevent money laundering may include amongst other activities such as

- minimum and maximum amount per transfer
- minimum and maximum amount per payment method and time unit
- daily deposit limit

- weekly deposit limit
- monthly deposit limit
- deposit limit per payment method (depending on the security of the payment method)
- prohibition of setting up more than one gaming account per customer
- prohibition of cross-country financing transactions (both deposits and payouts have to be effected through the country of registration)
- The account holder making a deposit must be identical with the account holder to whom payouts are made. According to international banking standards, banks refuse transactions in case of differences in the name of the recipient. Such payments are retransferred to the provider with a reference to the discrepancy regarding the account holder
- enhanced customer due diligence: From a defined amount (Money Laundering Directive: EUR 2,000); if a customer is included in a blacklist or PEP list, identification is mandatory. The gaming account must remain blocked until identification has been completed.

Enhanced due diligence includes, for example, the regular alignment with terrorism databases (e.g. UrU¹³ of GB Group) and the monitoring of unusual activities and transactions that deviate from the normal gaming behaviour of the respective player. Any activities deviating from the norm include for example unusually high deposits and stakes, deposits that are paid out again without any games or bets having been placed as well as the change of the means of deposit or payout. Players with several accounts and the use of one account by several players are also conspicuous.

Activities deviating from the normal playing behaviour of an individual player include the sudden increase in the stakes compared to the previous extent of that player's gaming or a sudden change of games or bets with an associated change in the stakes. Both games and bets as such as well as the processing of all master and movement data in case of online services are done electronically due to the nature of the system and therefore allow for immediate processing with regard to anomalies. Online gaming and betting providers are therefore able to automatically and efficiently check their customers' gaming behaviour by way of the data collected on games and bets and in this way to identify conspicuous players. Adequate cross tests and logic tests of master data allow for the detection of false information and conclusions can be drawn with regard to individual players by conducting random checks of gaming and betting behaviour.

4 Blacklist

Provided that a player uses accurate data when setting up a user account, conspicuous players may be blocked by deactivating conspicuous user accounts. In the process, the master data of the player to be blocked can be used as a criterion for identification. However, if a player, whose account has been blocked, sets up a new account using false data, it is possible to use at least the bank account required for paying out winnings as a criterion for identification. Because of the much further reaching options of identification, not least including external providers, it is possible to identify players with a high degree of reliability. This includes both the identification of conspicuous players (fraud and/or gaming addiction) as well as the identification of under-age players.

The most efficient way of blocking conspicuous players would be for all providers to use a joint database such as that of GB Group. Anomalies then would have to be reported to the database operator, with the result that all other providers would be notified. By having providers give feedback regarding conspicuous players, the quality of the database too would constantly improve. This approach would be analogous to that of credit information services and Schufa.

Comprehensive betting fraud blacklists by all providers should include not only detected or suspected betting cheaters, but functionaries and athletes as well. Providers could be required to compare registered customers with such lists to rule out that organisers, functionaries or athletes place bets on a sporting event in which they are actively involved. Most legislations provide this type of regulation for licensed sports betting providers anyhow.

5 Gaming Addiction

The traceability of gaming and betting now possible on the Internet is also used by research on gaming addiction. Anonymisation and authenticity of transactions constitute a clear advantage compared to conventional services such as casinos or betting agencies or to case studies, on which research on gaming addiction previously had to rely. Only very few transactional or customer data can be recorded with precision in a casino or betting agencies, if at all. In particular, automated recording and analysis of transactional data is not possible at all. Accordingly, the differentiated analysis options of online games and bets provide a valuable contribution to research.

With regard to problematic gaming behaviour various factors may be followed and logged throughout a customer's gaming activities. Irregularities, i.e. deviations from the norm, may be reported either by trained staff or by way of automated processes.

According to current research, indications of problematic gaming behaviour may be derived from the following factors and their development:

- duration of gaming activities
- frequency of gaming activities
- frequency of bets per time unit
- amount of stakes
- chasing losses
- non-adjustment of gaming behaviour

As already shown, the Internet makes it possible to track these factors with relatively little expense and mostly automatically. By recording every single gaming activity and transaction of customers from log-in to log-out, automatic alerts can be triggered through specific parameters or a combination thereof. In this way, it is easy to identify conspicuous gaming behaviour. (cf Hessisches Ministerium des Inneren und für Sport; Richard A. LaBrie et al.)

6 Bibliography

Pursch, Günter und Bär, Verena: "Sperrverfügungen gegen Internet-Provider"

Wissenschaftliche Dienste des Deutschen Bundestages, Berlin, 27.01.2009

Tanenbaum, Andrew: "Computer Networks"

Prentice Hall International; Auflage: 3

Rodewig, Klaus: "Netzwerke mit Linux"

Smartbooks Publishing AG, Kilchberg, 2006

Sieber, Prof. Dr. Dr. h.c. Ulrich: "Sperrverfügungen im Internet"

Max Planck Institute for Foreign and International Criminal Law, Freiburg, 2008

Hessisches Ministerium des Inneren und für Sport: Ausschussvorlagen HHA/16/115 und INA/16/58,

Drucksache 16/6024

Richard A. LaBrie, Debi A. LaPlante, Sarah E. Nelson, Anja Schumann, Howard J. Shaffer:

"Assessing the Playing Field: A Prospective Longitudinal Study of Internet Sports Gambling

Behavior", Journal of Gambling Studies DOI 10.1007/s10899-007-9067-3