Bachelor's thesis

Degree programme in Information Technology

2018

Robert Hernberg

FOLLOW THE MONEY

– Tools and tasks of fraud management in online money gaming

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

BACHELOR’S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2018| 41 pages

Robert Hernberg

FOLLOW THE MONEY

- Tools and tasks of fraud management in online money gaming

The Internet money gaming industry started booming during the first decade of the 21st century. By the end of the decade the competition for new playing customers and their money had become overheated. Operators fought for new customers at almost any cost and wherever there is money, there are fraudsters, too.

This thesis describes the money gaming environment from the point of view of a team focusing on fraud prevention at money gaming operators. It shares some experiences about designing, creating and implementing some basic tools used in screening and monitoring suspicious activities in the gaming system. It also takes a closer look at the process of handling suspect, fraudulent players and gives suggestions about streamlining, how to make this process more effective, efficient, and user-friendly to both the gaming operator employees and the playing customers involved.

This thesis is based on the author's personal experience in working for two different online gaming operators in two different countries, in two different decades.

KEYWORDS:

Internet money gaming, Fraud management, Usability, Database, SQL, Know your customer (KYC)

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Information and Communications Technology

2018| 41 sivua

Robert Hernberg

FOLLOW THE MONEY

- Nettirahapelien petoksentorjuntatiimien tehtäviä ja työkaluja

2000-luvun ensimmäisellä vuosikymmenellä internetin rahapelejä tarjoavissa palveluissa elettiin räjähdysmäisen kasvun aikaa. Vuosikymmenen loppuun mennessä kilpailu uusista asiakkaista ja näiden rahoista kävi ylikierroksilla: Pelioperaattorit haalivat uusia asiakkaita melkeinpä hintaan mihin hyvänsä. Ja aina kun rahaa on liikkeellä, on huijareitakin.

Valotan tässä opinnäytetyössä rahapeliteollisuuden toimintakulttuuria pelioperaattoreiden petoksentorjuntaan keskittyneiden tiimien näkökulmasta. Jaan kokemuksiani siitä, miten suunnittelin, kehitin ja toteutin joitakin perustyökaluja, joita käytimme seuloaksemme ja valvoaksemme epäilyttävältä vaikuttavaa pelitoimintaa. Tarkastelen myös sitä, kuinka mahdollisesta petoksesta epäiltyjä tapauksia käsitellään, ja kuinka näitä prosesseja voisi tehostaa ja ennen kaikkea tehdä käyttäjäystävällisemmäksi sekä asian parissa työskenteleville henkilöille että peliasiakkaille.

Opinnäytetyö perustuu omakohtaisiin kokemuksiin työskentelystä kahdella eri pelioperaattorilla, kahdessa eri maassa, kahdella vuosikymmenellä.

ASIASANAT:

Internet money gaming, Fraud management, Usability, Database, SQL, Know your customer (KYC)

CONTENTS

1 INTRODUCTION

The author started working for an internet money gaming service provider in 2007 with no prior knowledge about the industry at all. My role at the company service desk (SPOC – Single Point of Contact) dealt with daily operations, incident management, bug reporting. On occasion, the author was asked to take out most various reports from the gaming system database; those occasions soon became a daily routine, and as result the author became familiar wit the database quite thoroughly. When the Fraud Management Team was founded, the author was up to the challenge and immediately applied for a position.

Fraud Management Team, Security Department, Payments and Fraud, Consumer Safety – A beloved child has many names. Most people have never heard of these teams, and little do the know they probably have had had to do with one already at one point or another. Few people know what a Fraud Management Team does or who they deal with, let alone the tools of the trade. Some companies have multinational fraud teams with members from a dozen countries or more. It can be discussed whether or not a Fraud Management Team is always necessary, and what the bare minimum is or if we could make away with them altogether.

This thesis describes the basic internet money gaming environment, some tasks of fraud teams, and introduces an approach where a fraud team develops and tests simple tools for themselves to assist themselves in the daily routines, tools that can later be used as prototypes for more thorough in-house software development.

.

2 EXTERNAL TASKS

Some of the Fraud Teams' work is due to legislation or contracts with 3rd parties. Usually these would fall under the term Compliance. Naturally, it is the job of a compliance manager or a compliance team to see to, that all external obligations are fulfilled. The practical work then falls to those with best opportunities to serve this purpose. This chapter lists some of these tasks and reasons why these tasks often belong to Fraud Teams.

2.1 KYC

Identity check is known as KYC (Know your customer) in this industry. It is probably the most common task performed by fraud management teams in international online money gaming companies. Identity needs to be checked for various reasons. The requirements may vary depending on the jurisdiction under which the operator operates and the customer is located. These two are not necessarily the same.

Operators need to make sure the customer has the right to play:

Age: The customer needs to be of gambling age. In most countries this is, they have to be 18 years of age or older. Failing to check the age may prove expensive: In Malta, for example, the law (MGA. 2018.) stipulates that all money deposited by underage customers must be returned to them, irrespective of their wins or losses in gaming activities.

Citizenship, residence, location: The customer must be located in a country that does not forbid online gaming with the operator. The U.S.A., for example, forbids all online money gaming from its territory (FBI. 2007.) with overseas operators, and the operators are very careful to respect this, stopping any gaming activity from U.S. IP-addresses; For some reason, smaller countries' similar wishes do not cause same kind of paranoia. France and Spain, for example, forbid online gaming with non-licensed operators. In Finland, the customer needs to be a resident of Mainland Finland in order to play the national monopoly operator Veikkaus' online games.

National peculiarities: In Estonia, the population registry includes a parameter about the citizen's wish to play or not to play online. Licensed gaming operators need to check this upon signup, and act accordingly: Hefty fines are imposed if an operator is caught letting such persons play, who have in the population registry marked that they should not. In Denmark, similarly, the citizens can add themselves to a register (ROFUS) if they want to be banned from online gaming.

The residence or location of the playing customer may affect where the operator needs to pay the taxes, and how much. The residence or location of the playing customer may affect what kinds of gaming products the operator is allowed to offer and, what kind of marketing and promotions the operator can offer. Anti money laundering legislation requires gaming operators to know their customers.

2.2. Anti money laundering reporting

Similar to banks, insurance companies and payment operators, gaming operators, too, are obliged to know their customers and to monitor financial transactions and report any suspected money laundering or transactions with sums above a certain threshold levels to the authorities (Finanssivalvonta. 2010.) A failure in doing so may lead to legal prosecution. (Nya Aland. 2017.) The operator needs to appoint a Money Laundering Reporting Officer (MLRO) for this task. Very often it comes naturally that this is a person from a fraud management team.

In a perfect world, all gaming company employees dealing with playing customers would be aware of the issue of money laundering, and contact the operator MLRO whenever they encounter suspicious activity. MLRO would then investigate and make the decision about reporting. For gaming companies, however, the reporting obligation might raise a conflict of interest: Money launderers are possibly the best customers a gaming company can have. Reporting such a customer to the authorities might lead to investigation and a loss of a good customer. However, in 2014 in Finland alone, gaming operators filed 9100 money laundering reports to the authorities. To give the figure some proportions, the banks in Finland filed a total of 1125 reports during the same period. (KRP 2014. 8.) Nine thousand, one hundred reports is a huge number – one report may consist of many transactions. The money laundering reporting form on National Bureau of Investigation NBI (Keskusrikospoliisi, KRP) website does not look very inviting: Filling in different fields, many of which have little or no relevance with money gaming industry, about figures, transactions or suspicions that the user can hardly know or even speculate can feel like being interrogated for a crime one has not committed – as a suspect! Even if all the customer data from the company systems were available in a convenient format, it is not possible that all the reports would have been filed this way i.e. manually entering the information – not even any significant number of reports. NBI offers a possibility of submitting the information in XML-format, however. This leads to the conclusion, that one or more gaming operators in Finland are automatically filing money laundering reports, with most probably the same standard text and fields for each playing customer whose money transaction or sum of transactions exceeds a certain threshold level. Even when automatised, 9100 reports is still a huge number, which raises more questions: Have the gaming operators intentionally set the reporting threshold lower than required by the law? Would this be to make sure they always fulfil the formal requirements, the letter of the law with the easiest, simplest technical solution, or is there something more into it? Moreover, do the operators any longer really know their customers, as is the spirit of the law, if the systems file in a report based on one single variable, the money deposited.

2.3. Authority requests: Police, bailiff, social workers

Reputation is the most important asset of an Operator. The customer database is another asset. The customer database is confidential: Gaming operators do not reveal their customers' identities or activities unless to a competent authority, and only when so required by the law: The police may ask about deposits and withdrawals, the bailiff about customer account balance, for example. Even some social workers in Finland have been seen sending inquiries about their clients' activities, forgetting that they, too, have confidentiality obligations and no gaming operator would comment on such requests as they are not based on law – well-meant or not. In order to guarantee confidentiality, the task of the answering authority requests needs to be assigned to one team only. Confidentiality then means confidentiality both ways: The operator is often by the authorities requested not to inform the playing customer of possible police investigations or bailiff distraint orders. Often these tasks falls to the fraud management team; they are deemed to best know or find out the authenticity of such requests on one hand, and to find the requested data on the other.

Such is the confidentiality of a customer database that one gaming operator in Malta requires their new employees to sign an agreement, that the employee has to pay a fine of tens of thousands of euros to the operator if he/she reveals customer details to outsiders. The agreement also says that this fine can not be contested at the court of law. The reasons for confidentiality are self-evident, but worth mentioning: In different countries, areas, cultures and groups the attitudes towards gambling vary: In Finland money gaming is probably more acceptable than anywhere else: There are slot machines everywhere, and participating in the weekly national Lotto lottery happens even in many workplaces among colleagues. Even in Sweden, the attitude is similar, however, the public in general would probably not look well on a politician gambling away huge sums of money, anywhere. (Svenska Dagbladet. 2014.)

A customer database would be very valuable in the hands of another gaming operator. Such databases have legally changed hands against huge sums of money when, for example, Spain started to grant licenses for gaming operators and subsequently requires operators to have them: Only a handful of operators decided to continue activity in the country, the rest at least partly selling their customer data to the remaining operators.

Sometimes someone wins the jackpot – the winners in most cases prefer to stay anonymous.

2.4. Tasks due to contracts with 3rd parties

A fraud management team may be assigned the task of replying to external payment service providers' requests regarding fraud or suspicious activities. It is only logical, that a fraud team handles chargeback reports from payment service providers. They will always handle the chargeback information, because in this way, the information can be used by the team to track the funds, to search for possible related cases, and to learn about the behavior of suspect fraudsters.

Full service gaming operators seldom run all the operations themselves. Some, most or all the games can be run by external service providers. Poker and sports betting are the most common game categories run by external partners. In fraud related cases, the operator fraud management team contacts the external service provider fraud teams and vice-versa. Most cases involve identification verification and suspicious gaming activities in poker tables. Both the operators and the external service providers value quick response times in handling possible requests of stopping the funds where they are.

3 CUSTOMER ANALYSIS: KYC – KNOW YOUR CUSTOMER

3.1 Identity

The first chapter described the possible legal requirements of identity check. Identity check is not in place only to please the authorities, but it is also a cornerstone of all fraud management in its internal core tasks: We need and want to know who is playing. Unfortunately we can not ask all of the customers come by, show their ID at the headquarters. Identification needs to take place online. Do we then know anymore who we are dealing with?

National monopolies, gaming operators operating in one country only may have it easy: In Mainland Finland, for example, gaming operators use TUPAS (Finanssiala. 2011.) to identify online customers. Almost all identifications requiring strong authentication in Finland are done using this method, and most people are familiar with its use whether in banking, insurance or communicating online with government or municipal authorities. For them, it is only natural the identification is done this way upon sign-up. TUPAS supplies the operator with the name and the for each resident unique personal number. The personal number is then by the operator automatically checked against VRK system (owned by Väestörekisterikeskus, Finnish population registry) to establish that the municipality of residence of the playing customer is in Mainland Finland. It is highly unlikely someone would give away their internet bank usernames, passwords and keycode cards; Thus we can be quite sure that in most cases the playing customer is who they claim they are.

With gaming operators offering their services in several different markets, issues with identification turn more complicated: Operators can not accommodate for all countries' different personal number or identity document number systems – some countries have no identity cards, while in others having one and carrying it with oneself is obligatory – not all countries are willing to share their citizens' information, not to mention interfacing this with a foreign gambling company gaming system - and in no country would this come for free. What we then ”know” in the beginning is what the playing customer wants to tell us at sign-up. This is often where the Fraud Management Team and the Marketing Team will have their first fight: Marketing teams or teams responsible for the website front-end customer experience want to keep the sign-up as easy and short as possible. For the

Fraud Team, anything the playing customer enters can and in suspect cases will be used to evaluate the truthfulness of the rest of the information, and more than a bare minimum number of fields is a ”nice to have”. The bare minimum would be name, date of birth, language, country of residence, email address and a password – and maybe a mobile phone number.

3.2 One-account policy

Practically thinking all online money gaming sites have a one-account policy: One playing customer can only have one gaming account. There are several reasons to this: In some countries or jurisdictions, the legislation or the local money gaming license may simply so require. In order for Anti Money Laundering measures to be effective, one account policy is convenient: A player might try to avoid exceeding a money laundering detection and reporting threshold by using multiple accounts, which, unless somehow linked together would count as separate individuals (Kuustie. 2015, 15). In the same way, single account policy is needed by the operators in order to set effective limits to the number and amount of individual customers' payments and to prevent customers from avoiding these payments limitations: The restrictions are tight enough to stop any individual customer at any situation from causing excessive financial damage to the operator when making use of just one account. Limiting gaming accounts to one per person helps to keep sports betting professionals in bay, too: There are some to the gaming companies well-known professional sports betting experts, who know how to count odds and combinations of different betting products very well – all too well. The gaming operators want to limit these persons' bets and sometimes follow their activity closely to spot their own typos or mistakes in calculations - or ban them totally from sports betting and in many cases offer them a job. Money gaming is not a human right or allemansratt, and the operators, licensed or not, whether government monopolies or private, can still select their customers. A single account policy is needed also for the operators to prevent promotion abuse, players signing up several times to claim sign-up or other one-time, one-per-customer bonuses or offers. Also, many operators need to uphold some kind of responsible gaming limitations, in order to at least seemingly protect the customers from excessive playing: In Malta, for example, the operator has to close the gaming account if a playing customer confesses to a gaming addiction, and keep it closed. Under British gaming license, a gaming account must be permanently closed if the customer so says. Responsible gaming limitations are often in place to justify a government control or a total monopoly over money gaming: If a monopoly operator fails to show commitment in prevention of gaming addiction or limiting the problems caused by excessive playing, it gives a reason for the proponents of deregulation to strive for ending money gaming monopolies through EU common market policies, for example. And it is only smart to keep the customer database tidy even just for tidiness sake : We do not know for sure, for example, what is the basis of taxes or dues to gaming companies going to be five years from now: It is only good housekeeping to know how many individual customers there really are. For a serious money gaming operator wanting to learn about the past, to know the present situation and to predict the future, a well-enforced single account policy is a key to more accurate reporting, better marketing analysis and ultimately survival and success in the extremely competitive industry of money gaming.

There are very few exceptions to one-account policy: If a playing customer moves to another country, the old account must be closed and a new one opened due to taxes and other possible issues having to do with how the local legislation treats money gaming. The gaming account and payments currency might also need a change; having a mismatch here might lead into excessive payment service fees. Also, those accounts that have been opened by minors using a false date of birth must be closed, if the players want to start playing again once they are of age.

3.3 Payment methods

It is very important that the customers will find suitable and convenient payment methods in order to make a deposit i.e. to transfer money to the gaming operator's bank account, which would then show in the balance on the customer's gaming account. Gaming operators offer a variety of different payment methods: Online payments, offline payments, credit card, debit card, e-wallet, and paysafe card, to mention the most common ones. In the near future, mobile platforms will be widely surpassing desktop computers even in money gaming, and mobile payments such as Alipay are likely to become the most popular method. But this is from a security and costs point of view going to be comparable to online payments.

Online Payments

Online payment is by far the most convenient payment payment method from a Fraud Team point of view: In order to make an online payment, there must be sufficient funds on the bank account, and the person making the payment needs to know the login codes to the online bank and possess some other information, perhaps a keycode card, a security key or a mobile phone with a keycode app. It is the banking customers' responsibility not to reveal or give away these to any third parties, which makes these payments virtually risk-free to their recipients. Domestic online payments have a low cost, too. Online payments, however, require an uninterrupted internet connection to function instantaneously: The player starts from the gaming operator's payment page, selects the amount and the bank and gets redirected to his bank's online payments. After the necessary authentications, the funds are deducted from the player's bank account at the very moment of payment and the gaming operator gets this information when the customer is automatically redirected back to the operator gaming website, and the funds are added to the player's gaming account, even though the gaming operator will only receive the funds from the bank after a certain time the payment needs for processing. But if there is an interruption after the payment and the customer fails to get redirected back, the payment becomes an offline payment. In this case, the player's gaming account is first credited when the funds appear at the gaming operator's bank account with the relevant reference number.

Offline Payments

Apart from online payments getting interrupted, offline payments are otherwise almost obsolete in online gaming: They were used before online payments came into existence or into wide use. In an offline payment, the player gets a bank account number and a reference number from the gaming operator to use, and the funds will show up on the gaming account when the gaming operator receives them in a couple of days' time.

E-wallets

From the payment recipient point of view, e-wallets are a risk-free payment method: The payment service provider assumes the risk. This is reflected in very high service fees; How the costs are shared between the gaming operator and the player is up to the operator: Often the deposits would be kept free, but the number of free withdrawals might be limited to one per month, for example, and a fee would be taken for any subsequent ones. From a player's point of view, e-wallets are far from one-click shopping: Money first has to be transferred, normally from the player's bank account to the e-wallet before it can be further used. This may take several days. E-wallets are popular among players, who frequently use multiple gaming sites, however, because e-wallets are always there as a payment method, and payments and withdrawals to and from e-wallets are instantaneous, which further explains their popularity. E-wallet service providers also offer debit cards linked to the e-wallet, which makes it more convenient to the player. The most well-known e-wallet payment service providers are Skrill (formerly Moneybookers, a name that may suggest its popularity in online money gaming, especially odds) and Neteller.

Credit card payments

One sometimes hears people wonder why credit card payments are allowed in online money gaming at all – that one should not use borrowed money to unnecessities such as gambling. But the credit card is the most universal payment method: People all over the world have credit cards and they are being used to buy all kinds of goods and services everywhere, without judging whether they are necessary or not; That is what makes it so popular. Online, however, a credit card transaction is always a CNP (Card not present) transaction: The player can not show the card to the payment recipient at the time of the transaction. Because of the increase in risk, the fees for these kinds of transactions are likely to be higher than when swiping the physical card.

Debit card payments

Debit card payments are essentially similar to credit card payments, with the exception of Visa Electron cards, in which case there needs to be money on the account or an agreed overdraft in order to make a payment.

Paysafe Card

Paysafe card is a prepaid card used for anonymous online shopping. The cards are sold at various outlets in different currencies and denominations, and even online. The fees are high, currently up to 15% for low transaction volumes. (Paysafecard. 2018.)

3.4 Gaming behavior – Game categories

Gaming operators offer a variety of different kinds of games: Some are specialised in Poker (Pokerstars, Fulltiltpoker), or Odds (Unibet) – The biggest operators offer games from virtually all categories online games: Slot machines, table games, odds, poker, lotteries, bingo, to name a few.

Slot machines – a.k.a. fruit slots, fruit machines, the slots, poker machines, one-armed bandits are the cash cow of money gaming industry. The games are extremely popular: Anyone can start playing right away, because little or no skills are needed. Games come with dozens of different themes, different bet levels, different winning structures. Slotmachines are to the gaming operator risk-free: Their long term average return rate (theoretical payout percentage) is fixed, usually way over 90%. The biggest jackpots available in some slots are cumulative, which means that the amount paid out will never exceed that of the money reserved for the jackpot. Poker machines are in almost every respect similar to slotmachines - in distinction from online Poker games against real opponents, a very important distinction from a fraud team point of view.

Table games are the casino games that traditionally have, unlike slot machines, been played on a table. The most popular table games are Baccarat, Blackjack, Red Dog and Roulette. The individual stakes are usually higher than with slotmachines and the pace is somewhat slower. The rate of return and the best strategies for each of these games are well-known – And in the long run the house always wins: Card-counting or any similar fraudulent behavior sometimes reported from real-life physical casinos is not possible online.

Odds or sports betting is probably the oldest form of money gaming in the world, and it is nowadays not limited to sports only, but it is possible to play the odds on various other things, too, almost anything from entertainment to politics. Many online gaming operators are offering live odds, a possibility to place bets while an event is still taking place. The playing customers can then place bets on, for example, which team will score the next goal, or change their bet about the outcome of the game – with new odds and/or with a cost, of course. The fast pace of live odds makes the games more addictive and gives the operator the possibility to sell more products.

From a gaming operator point of view, offering odds is costly: The volumes need to be big, if odds are compiled in-house. Many operators choose to partly or fully buy this service from an external service provider specialised in odds compiling (such as Kambi). Even when buying the odds compiling service, the operator can still decide which products and odds to offer: The operator is responsible for handing the payments, bets and ultimately paying out the winnings. There are various websites listing the odds offered by different operators for different events and products. These are often presented as tables where it is easy to compare which operator offers the best odds. This makes the margins even smaller.

Poker is something that most people probably first think about, when money gaming is mentioned. In poker games, two or more players play against each other, and their decisions can and will affect the outcome of a game. From an operator point of view it does not matter who wins: Operator profits come from rake, i.e. the commission or fee for each hand played.

There are some operators specialised in poker games with in-house development of the games. Most operators, however, use external service providers (such as Microgaming, Bossmedia, OnGame) that take care of providing the gaming platform as well as connecting this with a number of other operators with playing customers so that they can all play against each other: The playing customers can then find games, levels and opponents they like virtually around the clock.

The most common types of fraud occurring in poker games are Chip dumping (losing funds intentionally to an opponent) and Collusion (two or more players are colluding i.e. collaborating against the other players in a multiplayer table by sharing information with each other or raising the stakes according to a plan agreed to in advance among themselves, trying to get advantage of the game this way).

3.5 Promotions: analysis, affiliate marketing

All gaming operators have some kinds of promotional campaigns in order to lure in new players to sign up, or to have the existing players make a deposit (into their gaming account) or to otherwise increase their gaming activity. Sign-up bonuses are often money bonuses, free bets, freespins, lottery tickets or gifts – or a combination of these. Activation bonuses – bonuses offered to all customers or to old customers that have not had recent real money gaming activity - can be any of these, or, for example, an opportunity to place a value bet on the player's favourite team on an important game. The operator may target certain groups or individuals and offer bonus codes. These can be unique for one-time use only or a general one-code-fits-all for a bigger audience, depending on the media (email, posters, leaflets, brochures, websites) and the kind of bonus. For money bonuses (a.k.a. bonus money) there is always a turnover requirement:

The player needs to bet the bonus amount a certain number of times in certain products before the winnings can be withdrawn, used in other product categories or transferred to (other) external gaming service provider games. Similarly, the possible winnings from slotmachine freespins or free sports bets usually have a turnover requirement before the funds can be withdrawn. What kind of bonuses the players make use of upon signup or when making payments tells a lot about them when assessing the risks they might pose.

Affiliate marketing is the most common way for the gaming operators to acquire new players. Affiliates in this case are the individuals or companies, which promote the gaming sites on their own websites or events. They might get a one-time fee for a new player signing up and making a first deposit, or a commission, share of the gaming operators' revenue from such players. Affiliates may offer new players sign-up bonuses as agreed to with the operator; These might vary from affiliate to affiliate and be more generous-looking and better suited to a specific market or population than the operator's usual offers. The players who come through an affiliate have this tagged to their gaming accounts; What kind of an affiliate it is might reveal something about the players. And of course, when there are affiliates, there is always a possibility for affiliate fraud, too.

4 FRAUD MANAGEMENT TASKS AND TOOLS IN PRACTICE

Life in a simple, small World would be easy: We would only operate in one developed country where virtually all the people are used to online payments and strong authentication in their everyday lives, and we would have access to the population registry of that country. We would only offer casino games – slotmachines and table games. We would not have promotional campaigns with money bonuses. We would not need worry about checking identity - it would be automatised and done upon sign-up. Payment risks would be non-existent; And no-one can cheat an online slotmachine. No promotions, no promotion abuse!

Few operators with gaming sites matching the above description exist. Big operators with their shareholders wanting more and more do not settle for just one market with a limited set of products. Life then becomes more complicated, little by little.

4.1 Identity checks

Different countries have different identity documents and different everyday practices of checking identity: In Spain, the modern ID card with a unique personal number (DNI) is mandatory and everybody has to keep it with them at all times. Until fairly recently Portugal had paper ID cards with the holder photo glued on and a fingerprint in ink. In UK, there are no ID cards at all: Those who travel, have passports, but otherwise the only document everyone has is the birth certificate. Identification is then often based on a recent household bill, which shows the name and the address, alone or together with the birth certificate. For this reason paper-shredders are popular items in British homes: One does not want to leave potential identification documents in rubbish bins for someone to collect. -It might come as a surprise to many, that the driving license is not generally accepted as an identity document in EU.

Because strong online authentication is not something people have access to in all markets, or the because operator deems an integration with such systems not feasible in a market, identity has to be checked in another way. The operator may request the identity documents: Some operators require the documents be sent by email, some gaming sites have a specific upload function for these. There are a couple of considerations, when deciding upon the solution:

-Responsibility for security and confidentiality: When submitting documents by email, the playing customer consciously assumes some risk and responsibility, when it comes to the security of their internet connection, email service provider etc. In contrast, with a document upload function on a website, the player has the right to assume, that the operator has taken the necessary safety precautions when it comes to the encryption when uploading and storing the documents on a safe (separate) server, with access limited to only those working with the documents.

-Images of identity documents need to be checked against the gaming account information, and the account marked accordingly: Which documents (ID, proof of address, proof of bank account holder, credit card, CCA-form, face verification) have been submitted by the player, which have been approved by the Fraud Team - or rejected and the reason for this. The information must be conveyed to the player, and it needs to be available to the Fraud Team, even Customer Support. The Fraud team might want to take another look at the images at a later stage.

-Initial implementation time and costs are in favor of the email solution: The inbox is already there at no (significant) extra cost. Planning, defining, designing and implementing an upload function takes time and occupies resources that could be used on activities that bring in money.

Company A used to work on an email based solution. But there was no designated field in the gaming system for the status of identity documents. When receiving an email with such documents, the approval of documents was marked in backoffice in a free form text field originally intended for customer support random notes (for which it was used constantly, too). The same text strings were used every time to mark the status and kind of an identity check, making it both understandable to everybody involved, and, searchable through database searches. The Fraud Team each time replied, sent an email to the playing customer signalling about the documents approval.

Company B made use of the upload solution. The playing customer would on the upload page see, which documents are pending approval (i.e. uploaded), and which ones have been approved or rejected. The Fraud Team would only need to tick the right checkbox, ”approved” or ”rejected” and in case of rejection, select the reason for rejection from a list.

Neither one was a perfect solution: Company A case, plain quick-and-dirty, though some might argue receiving a non-automatized email brings an extra personal touch to customer experience.

Company B case was not bad. But from a playing customer point of view, more of the available information could have been used to communicate the situation in the customer home page on the gaming site, at a (constantly) visible place: Most importantly, when documents are requested or rejected. This to avoid unnecessary strain on Customer Service and ultimately Fraud Team, which end up having to deal with questions that remain unanswered or of which the answer is not easily spotted by the playing customers. The reason for rejecting a document should have a free text field in addition to the few available options to better describe the problem to the player and to improve the success rate at a next upload attempt. The upload function had a filesize limit, of course, but it was set unnecessarily low, which resulted in players not being able to upload images taken with normal, modern mobile phones or consumer market digital cameras. – Frustrated with this or not knowing better, some players would end up reducing the image size to that of a postage stamp before upload: At Company B this led into an unnecessary argument with players, who insisted we zoom in to get the image bigger in order to see its contents clearly: Resizing an image and the consequences of a resize is not rocket science, but it is still far harder than playing slotmachines. From a Fraud Team point of view, a bigger image is always better: It is easier to point out manipulation attempts. There is no point for a filesize limit of, say, under 15Mb. Also, the player should (almost) in every case be allowed to log in with the right credentials even for documents upload only; even when all other functionality of the gaming account would for one reason or another have been disabled by the operator personnel. This is so that the documents end up in the right place and the account gets marked accordingly in every situation. (”Almost” here because of possible legal restrictions.)

Checking an image is very different from checking a real, physical identity document: Real documents have a certain touch and feel – even smell. 3-D prints, holograms and watermarks are not necessarily showing in an image. Real-life documents often change their appearance in UV-light and have an NFC-chip.

Fraud Teams have access to online catalogues of specimen images and information of different countries' identity documents: Both current and older versions. The images have the main security features introduced. The information may include details such as the normal validity period of the document, and to whom such documents are granted, and a description of the contents of the optically machine-readable field plus algorithms to count the checksums of such fields or scripts to do that online: Should there be a mismatch, the image certainly has been tampered with. Specimen images appear on many governmental authorities' websites, too, and the images can be used in many creative ways: Company A Fraud Team received at least half a dozen driving license images from different players in a period of a couple of months, all with the same face photo. They were all photoshopped, using an image the players had downloaded from a Swedish driving license authority website. Sometimes a Fraud Team would ask in good photos of documents rather than scanned images: These are more difficult to fake. And image files might contain metadata with information on the camera make and model, software, serial number, settings, time the image was created – almost anything, even the location. Of course this can be easily manipulated, too, but the data – or the absence of it - might sometimes help in decision-making.

Playing customer gaming account information entered by the player upon sign-up (or a later stage) is compared with the identity document data. This is not always as simple as it sounds: Different countries have different conventions when it comes to names and their use: In some countries only one first name is used, in others it is common to list all the given names. In Spain, both surnames (primer apellido, segundo apellido) are always used. This is an issue that should already be tackled with when designing the sign-up page and the databases, though no gaming operator will probably ever cater for each and every country's peculiarities. Another challenge is the transliteration of some languages into Latin alphabet: While the identity document information can be in Cyrillic only, for example, there are many ways people might try to transliterate their names. Experienced Fraud Analysts and International Fraud Teams with employees from different markets can usually spot attempts to go around the one-account policy, for example, players might try using different, from the norm deviating combinations of first and last names or their transliterations.

Sometimes there is an obvious mismatch between the information on the identity document and what the player has submitted upon sign-up. Was is a mistake or was it a deliberate attempt to cheat the system? -People do make mistakes, especially with poorly localized and designed websites: Dates are the most common thing, because they are written differently in different countries. It is upon the Fraud Team's best judgement and company policy to decide, how to deal with these accounts. Legislation, too, has its say: If a player had ”accidentally” signed up with a Malta-based operator while underage, the account would be permanently closed.

If the sign-up data in one or more markets contains a Personal Number (PN, SSN, DNI), this will help Fraud Teams to more easily distinguish between individual players. It is highly unlikely someone would make a mistake when typing their personal number, because these usually have one or more checksum characters, and a good interface would prompt the user to check the input value if this does not match. One might argue that giving a player the opportunity to sign up with an entirely false Personal Number would make it easier to detect fraud. The most user-friendly interface is, however, designed with honest players in mind: They are the vast majority. Fraud teams may have a manual online access to population registries to compare the sign-up data against these. In some very open societies like Sweden, these registers are available to virtually anybody – even identity thieves – which might complicate assessing the true identity of a player.

Proof of Address – The Utility Bill

It is a common practice, that the Fraud Team requests an image of a recent Utility Bill (electricity, water, gas bill, bank statement or an official letter) alongside with the ID. There are a couple of reasons for this: The Operator wants to verify the player address, residence, but identity documents seldom have the street address included, as in Poland. The Utility Bill also serves as an extra check about the ID: An ID can be valid for 5 or 10 years, even a lifetime in certain countries and circumstances. Asking in a recent Utility Bill helps make sure the ID is in right hands, not lost, stolen, copied, borrowed or inherited.

Face Verification

If there are further doubts about an ID being in wrong hands, the Fraud Team may want to do a Face Verification: Ask the player send in a photo of him/herself holding the identity document (usually passport) next to their face.

Phone Verification

Sometimes everything about the documents looks good or very good, but the gaming behavior is uncommon or has suddenly changed, especially in Odds. The player may then get a kind phone call from a Fraud Team employee or the Customer Service with a set of questions to verify, that it is really him/her, who has been playing. A phone verification may also be used, when players have lost their login credentials and/or access to their email account.

4.2 Payments

As is the case with identification, payments, too, are relatively easy to handle and implement, if the working environment is just one to the operator very well-known market with one predominant, safe, trustworthy and affordable payment method, such as online payments in Finland. Internationally oriented gaming operators, who want to scour in every penny from each and every potential playing customer in the World, however, do not have the luxury of sticking to one payment method only.

Credit card payments

From a Fraud Team's point of view, credit card payments can be a nightmare: Credit cards can be copied or skimmed – and the mere information on the card is in many cases enough to make a payment online: The card number, cardholder name, expiry date and cvc-code.

Online money games are a high-risk product in contrast with physical items purchased online, shipped to a certain individual with a known address with a few days' (or weeks' as in Finland) delivery time; Or airline e-tickets which are registered to an individual whose identity is always checked at the airport before the flight. In online money gaming the product is delivered instantly in a virtual form. Some kind of further risk management is certainly necessary.

An operator may choose to handle the credit card payments by themselves or make use of an external payment service provider. PCI DSS (Payment Card Industry Data Security Standard) dictates what is required from an online merchant in order to handle these payments. The standards are very demanding, reaching from what information about the cards and cardholders can be collected and stored, where, and how – down to the physical safety and surveillance of the premises and the server rooms. Fulfilling the standards might sound too tedious to a smaller operator; On the other hand, shouldn't these things be more of less in order, anyway, when handling huge sums of money and confidential information!

Credit card payment risk management is about adjusting risk scores: Certain actions add to the risk score, some actions more than others. If the risk score limit is exceeded, the payment will be rejected. It is important to find a balance: If one wants to get rid of all the risks involved, one does not accept any payments at all, but that is not very good for business. If one accepts all the payments with any cards chances are, that losses due to credit card fraud will be huge.

There need to be limits: How much money can be transferred and how fast: One must limit the amount (sum) per transaction and set a limit to the number of transactions per card per day. How many successful payments or failed attempts per card or IP can we allow for? How many cards per person? -Using a big external payment service provider may prove less risky than handling the payments in-house: They may have more data about payments and payment attempts from specific IP addresses and with specific cards: The risk score limit might have been exceeded elsewhere long before the first attempt with another Operator.

A few parameters in risk management have to do with location: For example, the cardholder country of residence, the country where the transaction is initiated (geolocation from IP address) and the card issuer country – and combinations of these: If all of the three in this example are the same, it would result in no added risk points. But what about a Finnish cardholder travelling in Sweden, USA, Nigeria or The Philippines? What is the likely risk and business impact? It is not necessary or hardly even possible to create a perfect matrix with all the different combinations; One can always whitelist individual cards, if a known high-roller happens to enjoy the holidays playing from an exotic location.

There are even security solutions counting the speed of the customer between transactions: If the geolocation between two transactions changes faster than what a feasible travelling time between the two locations would be, the transaction is denied. With the increasing popularity of VPNs, the likelihood of both false positives and negatives here needs to be addressed, when it comes to all IP-based geolocation data use: False positives through an addition in the gaming service Terms and Conditions for the players banning VPN use, and advising the players accordingly.

Credit Card Chargebacks

If credit card details end up in wrong hands, it may be used for payments online until the credit limit has been reached, or until the card issuer or payment service provider fraud team notice something out of the ordinary and gets the card cancelled – or until the cardholder checks their credit card bill and notifies the credit card issuer about payments they do not recognize. The cardholders can dispute any online credit card transaction made with their credit cards: The card has not been physically present, swiped, when the payment was made. If and when the credit card issuer chooses to believe the cardholder – they always do - they initiate a chargeback process: The card issuer sends an inquiry to the gaming operator with the payment details: Date and time, sum, reference, 4 first and 4 last digits of the card number and the reason code for the chargeback, most commonly ”Fraud (card-not-present)/No cardholder authorisation” or ”Transaction not recognised”. Unless the operator can convince the card issuer, that the cardholder has been the one using the card for the payment and that the cardholder has received what they were supposed to receive, a chargeback will take place, i.e. The card issuer will withdraw the disputed funds from the operator and the operator needs to pay a chargeback penalty fee for each transaction; If the number of chargebacks is very high, even penalty fines in order of up to $100 per transaction. The total cost of a chargeback may easily become greater than two times the initial payment.

To avoid chargebacks, the Operators may choose to accept credit card payments with 3-D Secure protocol only, or give negative risk points for payments using the protocol. The best-known implementations of 3-D Secure are Verified by Visa and MasterCard SecureCode. When using 3-D Secure protocol, the customer is after initiating the payment (by entering the sum, cardholder name, card number, expiry date and cvc code) taken to the issuing bank website for additional verification: This can be, for example, by SMS with a verification code to the customer's mobile phone, or by strong authentication using one time passwords. It is then very difficult for the customer to dispute the payment. 3-D Secure protocol is not cheap to implement as a merchant: The initial cost may be the final straw that turns the decision towards using an external payment service provider, unless the volumes are substantial. From a player point of view, 3-D Secure adds more complexity to the payment: It is no longer anywhere close to one-click shopping, but rather makes a credit card payment resemble an online payment. From an operator point of view this is not entirely bad, if it leads to players switching payment methods to online payments. But a thought of the credit card making Global mobility easy might go into shatters: SMS verification requirement renders the credit card effectively useless abroad, unless the customer's mobile phone deal allows for roaming.

When considering payment risk to the Operator, credit card payments are the only payment method really worth mentioning: With the other available payment methods the risk is on player or payment service provider side: The players are responsible for keeping their bank and other payment related credentials from getting into wrong hands, the banks and other payment service providers have their own responsibilities, based on laws and agreements. Adding other payment methods, however, adds to withdrawal methods – and risk.

4.3 Withdrawals

A vast majority of playing customers want to withdraw the possible winnings to the same place, where they made their deposits from. From the risk-averse operator point of view this is also an ideal situation: There is little point in anybody to commit a fraud while making a payment, and withdrawing any funds to the same bank account or instrument. In countries such as Malta, where online gaming is extremely regulated, the legislation, too, directs the operators to act in this way.

There are a couple of considerations, though: Online gaming is a highly competitive market, and timely withdrawals are one of the most important wants of the playing customers, a way for an operator to make a difference. Another one is the cost: Some withdrawal methods are to the operator more costly than others. And, most importantly: Not all payment methods, instruments or their implementations allow for withdrawals.

There are several likely scenarios which all will happen, if there is a to the playing customers a free choice of from each other totally independent payment and withdrawal methods, without limitations to transfers:

Money laundering at its simplest form will happen, for example: A customer deposits 10 Euros from Bank Account A and 10000 Euros from Bank Account B to his gaming account. He withdraws 10010 Euros from his gaming account to Bank Account A. The money is now clean: The customer may claim he won a jackpot at the online casino with a bet of 10 Euros. The operator suffers the transaction fees and possibly gets sued for assisting with money laundering.

Credit Card Fraud will happen, for example: A customer deposits 200 Euros to his gaming account using an unsecured credit card transaction. The card used was a copied, skimmed or stolen one. He then withdraws the funds to an anonymous paysafe card. The operator suffers the transaction costs and possibly a chargeback with the chargeback fee involved.

In the case above, the card does not need to be a stolen one: The customer may use his own, unsecured card and decide to dispute the payment, initiate a chargeback procedure; For some mysterious reason unknown to me, this would be called ”Friendly Chargeback”.

Transfer from a credit card to another instrument will happen, for example: Banks would charge a service fee plus commission (2 Euros + 2%, for example), if a customer wants to withdraw money from their credit card to their bank account. However, there is no service fee for the customer, if they purchase services or products online with the card. The customer makes a deposit of 1000 Euros from the credit card to the gaming account. From a bank point of view this counts as a purchase of gaming services. The customer then withdraws 1000 euros from his gaming account to his bank account. The operator suffers the transaction fees.

Similarly to the case above, a customer may want to speed up a transfer of funds from an e-wallet to his bank account or go around the possible service fees using the gaming account in between.

Ultimately, some customers will try start using the gaming service as a bank, paying their bills, debts, whatnot, from their gaming account to various payees' bank accounts. In this case, the transaction fees are just a tiny fraction of the losses for the operator: Administrative costs will outnumber them easily, when Customer Service, Payments and Fraud Teams are trying to figure out what went wrong, when a customer says his friend claims not tho have received the money the customer sent from the gaming account to the friend's bank account the other day. Not to talk about Payday loans' a.k.a. Quick cash loans' funds appearing at the operator bank account without any indication to which playing customer gaming account they would belong to.

To avoid the above scenarios, all gaming operators state in their rules and regulations in one way or another, that deposits should be done in gaming purpose only. In practise, the player should bet at least a total of the sum of the deposits once before requesting a withdrawal. Otherwise the operator would impose a fee to cover the costs.

Sometimes the payment method and instrument used for a payment are not available for a withdrawal: Some cards or card issuers do not allow for this or the card might have reached its expiry date. An e-wallet or a bank account may have been terminated. In these cases, typically, the operator asks the player to withdraw the funds to a bank account: The player needs to enter the sum to withdraw, IBAN and BIC and the name of the bank account holder. In some countries and banks, these need to match, otherwise the transaction will be rejected. This can be very strict: In China, for example, even the case needs to match for names written using Latin alphabet: If the name at the bank is written with all upper case letters, that needs to be the case with the withdrawal request. In Finland, so far, this is not necessary: Any string looking like a name will probably do. This is not a challenge just for the Fraud Team, but for the occasional customer, who types in a wrong account number. If an account with a given account number exists, the funds will end up there, whoever the account belongs to. If no such account exists, the funds will be returned to the operator and the Payments Team will need to manually put them back where they belong.

Optimally, the player side user interface would always suggest only withdrawal methods, instruments and amounts that match with the payment methods, whenever available. But truly international operators have a number of constantly changing payment methods, and each change comes with their implementation cost and time. Integration teams' resources are often very limited, and downtime is expensive. Everything is a compromise: If it weren't so, there would be little use to operative Payments, Fraud or Customer Service teams.

4.4 Gaming behavior

Truly international gaming operators, who want to scour in every penny available in the World shall also provide most games, of all different categories. Casino games, especially slotmachines are the cash cow; offering other game categories is often as much a means to bringing in more customers to play these as it is for the profits from the games themselves.

Poker

Typically, a big operator would offer poker games through a couple of external service providers (ESP). These ESPs, in their turn, offer their services to a number of gaming operators of which the players then would find games, opponents and levels of their liking.

In order to play, the player needs to transfer money from the gaming account at the gaming operator to a poker wallet at an ESP. Depending on the operators and ESPs, this can be done manually for a player selected sum, or automatically with the full gaming account balance (a.k.a. ”seamless wallet”). Similarly, depending on thedoesn't technical solution, the player can transfer money from the wallet at an ESP back to the gaming account or the account balance is automatically kept up-to-date.

In poker, the players can with their decisions and actions affect the outcome of a game: It may not be possible to win every time at will, but it certainly is possible to lose every time. Losing money intentionally (usually to the player known person) a.k.a. Chip Dumping is categorically forbidden on all online poker sites. At first glance losing at poker tables does not sound like a smart move: For why would the Operators or Fraud Teams be interested in someone wanting to get rid of their money! Losing money, however, means that another someone is going to get that money - that money minus rake. (Despite conspiracy theories, the poker operators do not need to employ people to anonymously or with varying aliases to play, win money for the house. The house just gets the rake, which is basically a commission for organizing the game. It is for the house irrelevant who wins a game – the house always wins, gets the rake, anyway.) This opens a new path for the money to flow: The money is no longer bound to one Operator, but the funds lost by a player from one Operator can later find their way to another player's gaming account at another Operator, perhaps in another country, with their own set of payment and withdrawal methods, and routines for identity checks, screening and monitoring.

It is possible for the ESPs and even Operators to monitor the games in real-time. With hundreds or thousands of hands being played at any moment, there is little use to this feature by itself: Any monitoring needs to be automatized and triggers set for automatic actions and alerting the Fraud Teams.

Loss-per-hand is the most often used metric: How much money per player per played poker hand is being lost. The monitoring systems automatically calculate this for every hand, and take action, if a threshold is exceeded: Send a report to the ESP Fraud Team and the Operator Fraud Team for checking. Most cases are blatantly obvious, but sometimes a manual check monitoring the player activity by watching a game live or studying through the playing history hand by hand in search for signs of chip-dumping might prove difficult: Not every case is sky-clear: It is not always easy or possible to identify, whether the intention has been chip-dumping, or if someone is just very bad at poker. Creating AI for something that is this much dependent on human behaviour or psychology is unlikely to succeed at this level. If the players involved in chip dumping are cunning and more than the usual two, the funds could easily vanish from a river into smaller streams, soon beyond reach. The funds can in the end be gathered again back together from the smaller streams, under radar: If the perpetrator or the perpetrators are very patient using ”players” in different geographical locations, operators, IP addresses, ISP:s and computers, it is possible that they may succeed in avoiding detection: However, a tiny mistake with any of the above may reveal the whole plot.

A better but more complicated approach to following the money would be tagging the funds to the players at entry points of the poker ESP: In this way, we would always know how much and what proportion of the funds of any player originates from a certain other player, whatever the way or method it got there: This could in its turn be compared to the number of hands played, how long ago the player registered or any other relevant or interesting parameter. If the check is only executed upon a transfer request, we could avoid false positives and much of the unnecessary manual checks and monitoring. Of course it is totally up to the Poker ESPs to decide on their level and methods of detecting and reporting chip dumping: It is just another feature among many others that the Operators may need to consider, when selecting suitable ESPs – Probably way down, close to the bottom of the shopping list.

Poker together with credit card payments is an extremely dangerous combination: Funds from a credit card payment at one operator can be chip-dumped to a player at another and withdrawn in a minute, if no checks are in place. Even with them, information flow between Operators' and ESPs' Fraud Teams is often too slow to stop the funds before it is too late, and an occasional hit-and-run chip-dumper might well succeed. At Company B, each new player had a Poker Loss Limit, a specific total sum, amount that a player is allowed to lose in Poker. This limit would only be removed or raised if payment methods for the player are limited to the safe and secure ones – such as online payments – or after a thorough identification and signing of a CCA form. When talking to poker players, asking them about their success, practically all players claim they are winning players or at least around break-even. The first situation in which they need to confront the truth is when they hit the Poker Loss Limit and contact the Operator. Fortunately, this is a much more common reason for a customer contact than any fraud suspicion.

Obviously, similar risks are present with any multiplayer games where the players can significantly affect the outcome.

Identity checks, screening and monitoring done by operators function quite like security checks at airports: Once you have passed the security check at one airport, it is possible you may not need to go through another one, because of mutual trust between some airports. Similarly, there needs to be some kind of trust between operators and ESP:s about the origin of the players and their funds. And if an operator is too lax with the security checks, chances are they will one day suffer a hit themselves, getting an unsecured credit card payment of their own player chip-dumped to another of their own players and withdrawn.

4.5 Promotional campaigns

Getting new customers and keeping the old ones active is the single most difficult thing about online gaming. A big international operator is big only, when it has many active playing customers. How many? -The CEO or the spokesperson of the Operator would most likely say the number of their active players a business secret. A business analyst would ask you to define an active player: It must be someone who deposits money to the gaming account and plays the games. Depositing alone brings no gaming revenue: If the player happens to pass away right after making a deposit before playing, for example, the inheritors may still insist the funds must be returned. (In fact, one gaming operator in Finland already has the necessary technology, integration in place to automatically pay out the remaining funds and close the gaming account when the population registry shows the player is deceased.) Theoretically, a winning poker player could bring in revenue without any deposits but the first one, but these cases are marginal. As a Fraud Analyst the author would say an active player is someone who still plays, has made a second deposit and who has been identified. But there are as many definitions as there are people; This may depend on how the figures are used, is it for really describing the success of a marketing effort in order to learn and to evolve, or is it to fulfil some expectations of a balanced scorecard system affecting the possible bonuses of the employees, management and board members involved.

4.6 A free lunch

Just like with any other services, gaming operators, too, advertise special offers for new customers. Because the industry is highly competitive, the bonuses for an initial deposit at sign-up are sometimes very lucrative, one-per-customer offers.

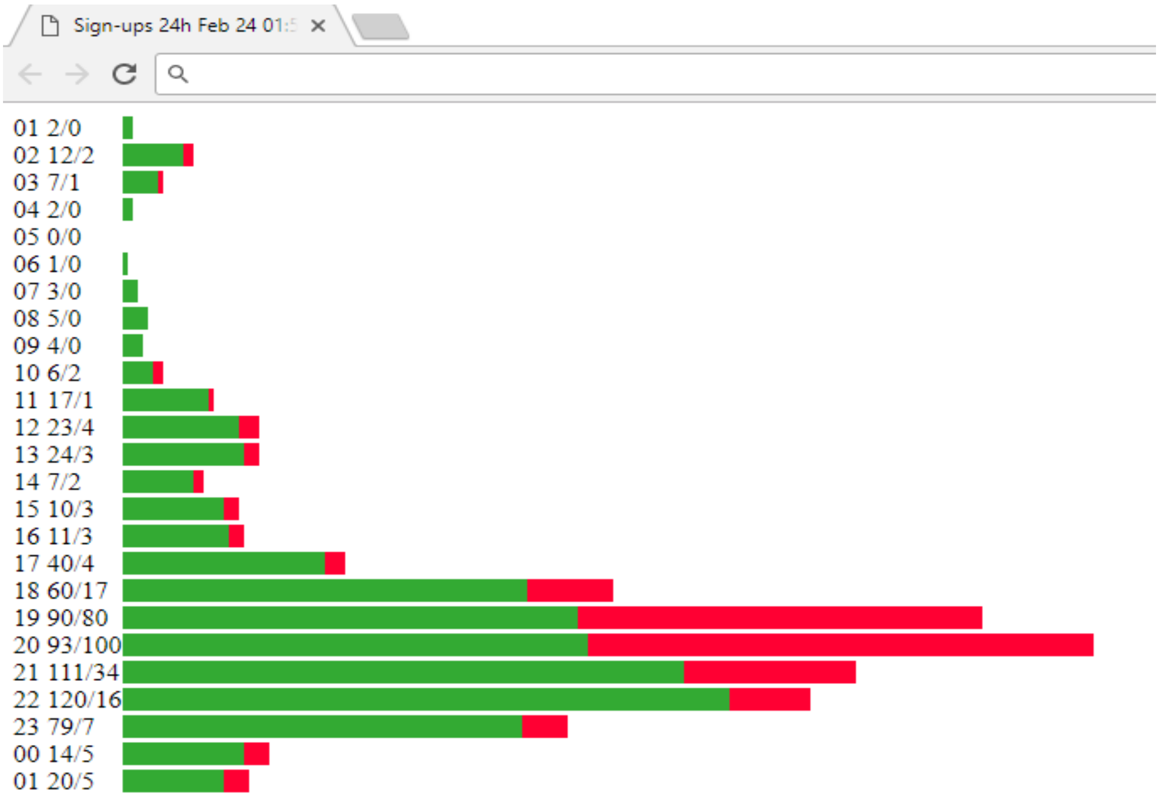
Company A used to have very good offers, for example a 10 euro bonus for a sign-up with no deposit requirements, with a minimal turnover requirement of just one time. This was a free lunch: Any new player could play with the 10 euro bonus money and make a withdrawal of his winnings. This resulted frequently in people signing up several times with varying false or stolen identities. The only obstacle was the one-gaming-account-per-player policy, and the Fraud Team enforcing it. For if a player has an infinite number of 10 euro bonuses available, there are two basic approaches to getting a free lunch: The first one is playing to the player high-risk-games, such as slotmachines: If he gets a bigger win, he would try, withdraw the winnings into his bank account. Of course there is a possibility of never hitting anything close to a jackpot, given the finite time. The other approach is playing to the player low-risk games, such as table games: Placing the bets correctly on Roulette (black+red+0) or Baccarat (dealer+player) would always yield a return of more than 90%. One could sign up 100 times and have a total of almost 1000 euros on 100 different accounts. However, withdrawals in this case could prove difficult: The gaming system would not allow for the use of the same bank account number more than once, and few people have dozens of bank accounts. (Some creative individuals discovered, though, that one could add an arbitrary number of zeros in the middle of a Finnish bank account number, and the gaming system would treat these as different bank accounts. Later, with the introduction of IBAN, this was no longer an issue.) But there was still another way for getting the funds out of the system: Poker – the external service providers. The players could transfer their winnings to poker and through chip-dumping, gather all the funds into one gaming account, possibly at another operator, before a withdrawal request.

4.7 Basic Screening

Obviously some screening and monitoring was needed to understand the scale of the issue and to intercept possible fraudulent transactions. However, the gaming system had been built mostly with honest players in mind. The only tools available had been developed for the use of a Customer Service Team: A backoffice with basically a view to one individual player's information at a time only, and the widgets to manage the gaming account. Coming across promotion abuse this way by accident or even intentionally would first happen when it is massive or blatant: Player names or patterns that have become familiar to someone in the Customer Service, Support or Fraud Team due to the abundance of the similar details; Or just because of truly obviously bogus personal details: Random strings, celebrity or cartoon character names, phone numbers repeating the same digit(s). But any real-time information on the doings of multiple players' was only available through a PL/SQL command line interface to the gaming system database. While an SQL command line interface is extremely effective when one needs to find and combine any data in the underlying database, it is not very user-friendly for much else. Using it for screening purposes, especially, is not sustainable at all: No team can employ people full time running just one script every minute or two or five. And while command line interface output can be quite descriptive – depending on the selected queries - it still needs far more than just a glance to analyse the results, because it lacks any visual clues. Usability needed to be addressed: We needed something automatized, not manual. We needed something highly visual that could be interpreted in a fraction of a second, something not to constantly observe but rather to attract attention when necessary.

There were not enough resources to make a system recognize bogus identities or to learn similar patterns of players' signup information. It is not certain that such a system could ever be built either, for these are sometimes very difficult for even us humans to distinguish, largely a matter of language and cultural background as well. This meant the initial screening needed to be based on something else but the information filled in and submitted by the players upon sign-up. The very first prototype for screening was therefore made based on players' IP addresses used upon sign-up: Naturally, the gaming system database had always had information on each player's IP-address as well as sign-up time. This data was enough for a histogram that would show sign-ups per hour. On y-axis the time, the hours of the day going 24 hours back, on x-axis a bar showing the number of sign-ups, new playing customers on each hour. The bars would come in two colours: To the left, the green part of each bar would represent the number of unique IP-addresses players used upon sign-up i.e. sign-ups more likely to adhere to the one-account policy. Topping the green part of each bar, the red part would show the number of sign-ups from non-unique IP-addresses, i.e. if more than one sign-up would come from one IP-address. Colours here are easily distinguished and the generally, culturally accepted ones: Green and red, good and bad, allowed and forbidden. (In larger teams with possibly changing personnel, blue could be used instead of green to cater for the most common type of colour blindness.) 24 hours back was selected, because one could then easily observe the normal situation and flow and distinguish any sudden or gradual deviation from it, be it the number of overall signups or the non-unique IP ones. Any member of the team could from the screen instantly tell, if there is a suspect promotion abuse going on (lots of red), whether the number of signups is in the increase or decrease (bars longer or shorter than the previous ones) – or if the system is down (no bars). What is more, no-one really needed to be staring at such graphs: One could simply not help noticing the possible presence of red colour, especially in large quantities. Even random visitors, passers-by would ask: Is there something going on with so much red on the screen?

Because the necessary data was already available in the gaming system, no extra resources needed to be assigned: One table of its Oracle databases stored, among other things, each player's sign-up time and sign-up IP and a for each player unique customer ID. A short PHP script (on an odd server somewhere at the corner of the server room) would create a database connection and fetch the data with a simple SQL query and draw a HTML formatted page, table with the histogram bars. The page would refresh itself every 60 seconds. The database required username and password were not stored in the script itself, but prompted for by the script as a username and a password which then were used to access the database. Upon a successful database connection i.e. when the credentials were approved by the database, the script would initiate a session storing these as session variables, thus eliminating the need to request them again or to store them anywhere else. This way, only persons having access to the underlying database could make use of the script and the information it provides. Such persons would also know the implications of initiating an SQL query, specifically the implications of running a heavy one too often by refreshing the view constantly or in a rapid succession.



```
01 2/0
02 12/2
03 7/1
04 2/0
05 0/0
06 1/0
07 3/0
08 5/0
09 4/0
10 6/2
11 17/1
12 23/4
13 24/3
14 7/2
15 10/3
16 11/3
17 40/4
18 60/17
19 90/80
20 93/100
21 111/34
22 120/16
23 79/7
00 14/5
01 20/5
```

Figure 1. Sign-ups per hour.

Figure 1 shows the very first prototype of screening. In general, most activity at any market appears in the late afternoon and evening local time, with a tiny peak during lunch time. In this figure, everything looks like business as usual until 17 o'clock (17:00 – 18:00): During that hour, the number of signups increased more than usual, which might signal a beginning of a promotion, but could still quite fall under the usual variation. After 18 o'clock, however, the number of signups increased sharply and at this point it was obvious that a promotion had started. After 19 more and more red colour shows, indicating that not all the signups come from different, unique IP-addresses: Promotion abuse was ongoing: Probably a poorly designed campaign or campaign codes leaked to a web-forum – or both. Of the signups between 19 and 20 o'clock, 90 came from unique IP-addresses and 80 from non-unique IP-addresses. We can not from the graph tell, if these 80 non-unique ones all came from one IP-address or if they came from 40 different IP-addresses, or something in between; The database query is simple, fetching only the number of signups and the number of distinct IP addresses each hour. The length of the whole bar shows the number of total signups, the red part is simply the difference between the total signups and distinct IP addresses used upon those signups. But this information was enough to give us a relatively early warning to start monitoring and eventually discontinue the promotion.

Screening based on IP addresses was a success: On several occasions unusual activity was detected this way and further action could be taken. Even though it is possible for the prospective player to change IP-addresses, it requires some effort, more work, an extra step further away from 1-click shopping. But even in the richest countries in the World, there are people to whom a 100-euro extra income every now and then would feel significant, worth some time and effort – not to talk about the poorest where this might present a monthly salary, something for the truly international operators to keep in mind. The World is evolving, and the fraudsters are, too, and the gaming operators need to follow.

Once the first screening system was up and running, it was easy to add any lists, histograms, line graphs or pie charts: PHP has great features for creating images on the fly, and the programmer has a full control of the canvas, pixel-by-pixel. This makes it possible to squeeze a maximum amount of information into the screen space available and adjust everything for the visibility of anomalies. Some charts proved more useful than others. A pie chart with sign-ups by country would give a general idea about where things are happening on that specific day. A list of signups with a mismatch in geolocation, i.e. when the user selected country differs from the country their IP address indicates could reveal identity theft or identity misrepresentation. Rather than country names, the national flags proved to be a good colour coding, easily distinguished from afar. Tiny line graphs for each currently active promotional campaign showing campaign codes usage as a percentage of the total available codes over time; A sudden change in activity could need some extra checking. Bar chart with recent credit card payments, the focus on payment status, the proportion of rejected or non-captured payments of the total: There is always a reason for a rejected credit card transaction, and one of the reasons could be a fraud attempt. If the chart would indicate any greater number of rejected payment attempts, Fraud Team could start monitoring the situation more closely. The chart, however, proved even more useful to the Payments Team: If a large number of payments stayed initiated, not updating into captured or rejected, this would indicate a situation when there is a technical issue somewhere. The chart helped to notice this before any bigger number of gaming customers would experience delays or failed payment attempts and start calling the Customer Service. Most of the time, Payments Team contacting the Payment Service Provider and notifying them about the issue helped. Not to talk about long term effects such as reputation, but an early warning and an early solution to a temporary issue like this directly effects the incoming deposits, even for a certain time afterwards: As described earlier, one of the credit card risk management parameters is recent payment attempts; if the accepted level is exceeded, any new payment attempts would be rejected within the specified time interval. Risk management rasters can not cater to every possible situation: In this kind of a case, even if the reason for rejection was a system error, the number of attempts would count irrespective of the result, and payments from that card would be rejected – leaving the playing customer without an opportunity to place bets and the operator without an opportunity for a profit.

Recently there has been a lot of discussion about online shoppers' privacy, about how different trackers are trying to gather information on shopper behavior online in order to establish what kinds of products and services they are interested in and at what kind of prices these could be sold. Browsers are being equipped with add-ons such as adblockers and users growing more wary about the situation may switch between browsers or opt in using browsers' anonymous state to avoid tracking by cookies. At the same time, virtually all web pages have some Java or Flash content, and it is widely speculated, that trackers are capable of using these in order to identify each device using the features of these instead of cookies. And it is not merely speculation.

Iovation

Iovation has been using a technology similar to the one described above for years, though not for marketing purposes. It offers a product to online merchants with a device-based solution very popular among online gaming operators: Customers visiting the operator gaming website automatically run a script from Iovation, that gathers information on the customer's device. This information is then used to calculate a device fingerprint hash, ”black box”, unique to each device that can be linked to one or more customer accounts at the operator or other operators.

The iovation black box can be used to share information between operators about devices with suspicious activities of different kinds: An operator detecting fraud can at Iovation tag the black box with a relevant code, anything from Credit Card Chargeback, Identity Theft or Chip-Dumping to Promotion Abuse. This way, no confidential customer information is leaked: No complete lists of black boxes are shared but only those that are included in the relevant operator customers' devices are available to each operator. But the other operators' Fraud Teams get a warning if the same device is used at their gaming service and they can take the necessary measures.

The black box can be useful by itself, too: As in the above case of screening sign-ups per IP-address per hour, sign-ups per Iovation black box would produce a more exact result. This has at some Operators been used even to automatize one-account policy enforcement by locking accounts, when the number of sign-ups from one device exceeds a certain figure. Nowadays this is well justified as most devices are personal, never shared with anyone at least not for money gaming purposes. Five, not to talk ten years ago, however, this was not equally self-evident, and one operator's Marketing Team felt there would be a risk of losing ”prospective active players” this way. Of course this choice – whether or not to automatically block accounts - would affect the resources and the type of work needed at the Fraud Teams: Not having it automatized means more screening. Having it automatized, with possible false positives, results in more prospective playing customers getting a less than perfect initial user experience at the operator, in best case contacting the Customer Service and getting their case reviewed by the Fraud Team. And in worst case, moving on to another operator.

Now if a lack of variety in IP-addresses or black boxes can reveal a fraudster signing up, creating multiple accounts, so could the abundance of either of them: If every sign-in to an account happens from a different IP-address or shows a different device black box, that most certainly raises suspicions, too: There might always be an overly eager Fraud Team member wanting to go through accounts where the number of distinct black boxes is equal or close to equal with the number of sign-ins: It is not very common for people to switch between devices every time they sign in and play. A successful fraudster would need very good record-keeping, seeing to that these are consistent at all times: One gaming account should make use of the same IP-address or few IP-addresses and black boxes. The fraudster should never forget to switch between these when switching accounts, no mistakes allowed: Using the wrong IP or wrong blackbox in association with another account would quickly reveal it all. If you want to be a good liar, you need to have a very good memory.

The best efforts of fraudsters of this kind so far are making are some automatized systems signing up, consistently changing IP-addresses and blackboxes. At the same time, everything a player or the system he created enters, can and will be searched: If 1000 players give the same answer to the secret question, their password hashes are identical and the length and pattern of the email address is the same, they have been lazy, and they will be caught. At best, it is more like a sports for any Fraud Team to reveal these, a very good exercise to learn the creative ways of people and the features of the gaming system and at the same time a chance to prepare to fight possible more serious fraud. At its worst, it is a very inefficient way of fighting petty fraud with little economic impact.

4.8 Monitoring

When screening reveals something out of the ordinary, interesting from the Fraud Team point of view, they start monitoring the players indicated to judge whether the activity might be fraudulent. In this case ”players” often translates to ”gaming accounts”, for the odds are we are not talking about individuals behind the gaming accounts, but often an individual with several accounts. At company A, just as with the case of screening, the available tools were not really fitted for monitoring purposes, either: The players, and the Customer Service Team assisting them when necessary, need to have access to their sign-up information as well as gameplay and other monetary transaction history, gameplay by gameplay, transaction by transaction: This is in order to ensure transparency and fairness, that the players get a result and a possible win of every single gameplay they pay for, and that every penny is being accounted for.

The players can see their own details when logged in to the gaming site of the operator, Customer Service Team can see one individual customer's details at a time in the gaming system backoffice. The needs of a Fraud Team are quite different: First of all, Fraud analyst probably wants to see, compare several gaming accounts at the same time, the focus on the customer-entered details and other information acquired when the account has been signed-up or signed into. These accounts might be, for example, those that have several other accounts signed-up for from the same IP-address or device, that initial screening has revealed: The red part on the bar graph of our initial screening prototype described above. Selecting such accounts (clicking the red part of the bar working as a link) would show the customer ID, account balance, sign-up time, Name, street address, customer entered country, IP geolocation country, phone number, date of birth, email address, answer to the secret question, aliases used with external gaming service providers, some of the (otherwise too long) password hash, and the number of IP or blackbox associated accounts – all of these as columns, one account per row. From the information formatted this way, it was relatively easy for a Fraud analyst to notice, whether such accounts have been created by several distinct individuals or by one person only: The length of different strings in these fields alone can be revealing, if the email addresses are all of same format, for example. In general, a lack of creativity is a most revealing thing, something that can not be assessed by machines, but needs a Fraud analyst, preferably a person with the right cultural background, some knowledge of the language and perhaps even experience. In this example, in the column showing number of IP or black box associated accounts of each player, that number was a link opening a view with those accounts, leading possibly to even further revelations, fully punishing the fraudster for any laziness or mistakes. Another difference between the Customer Service needs and Fraud Team needs is related to the way the transactions are shown: Instead of a long, timestamp ordered listing showing possibly thousands of gameplays and some payment transactions, the Fraud Team initially needs to see just a summary: Payments (euro sums) in and out per payment method, bets and wins (euro sums) per game category, last 30 or a selected number of days.

The above are just examples of simple systems and variables that were and can be used for screening and monitoring, some of the tools that the author made to help with the everyday workflow, hopefully prototypes for future in-house developments. Similar (close to) real-time graphs or information displays are available in many well-known, commercial products, such as Splunk (Splunk) or Oracle RUEI (Oracle).

4.9 Stop the money

The tools developed by the author helped us greatly in screening and monitoring, even though the tools were all about just showing the existing gaming system database information in a different, more usable format. They helped us to reveal in total a huge number, an enormous amount of accounts with something suspect. My tools made use of barely reading data from the database, because we had read-only access, which is self-evident: The number of people with command line database write-access must be restricted to a bare minimum, and any systems with write-access must be thoroughly tested and approved which certainly was and could not be the case with screening and monitoring tools constantly adjusted to cater for the daily needs by a self-learnt PHP/PL/SQL experimenter. But, just reading data from the database can not stop the fraudsters – unless one reads so much and so heavily that the whole system goes down, which is not exactly an optimal solution.

The HTML-based backoffice used by the Customer Service and Fraud Teams, however, had the necessary functions to activate, block or to close gaming accounts of individual customers: Log into the Backoffice; Search customers by name, email address, customer ID, phone number, personal number etc.; Select the account(s) and the desired account status change from the list; And submit the HTML-form; Done. The problem was, that the suspect accounts could run in dozens or hundreds. And one fraudster's numerous accounts did not necessarily have anything by the backoffice searchable items in common in order to have them appear on one and the same backoffice HTML-page, with just one form to check and submit in order to block the accounts and stop the thief. Thus, it was definitely not feasible to block all the suspect accounts one-by-one using this system.

The existing HTML-based backoffice was quite simple, however, and it was relatively easy to recreate similar pages and views with exactly the same form and field names. The author noticed, that once he logged into the backoffice, the system did not check the origins of the data, and the author could submit a form from a page created by myself. This way, using a PHP-script from the screening and monitoring tools to fetch the data from the database, the author could have it create an HTML-page and populate a form in it that would look like backoffice search results with that data and inject the data, submit it to the system for account status changes, dozens of accounts at once. The system should naturally check, that the form submitted data would be in a right format and go to the right place. This kind of reverse engineering gave an opportunity to use the existing backoffice as an interface to write or to modify certain columns or rows – the ones containing the related data included in the form of the bogus backoffice page - in the database in a safe manner. This way, we had a tool to change the account status: Block, close or activate any number of selected, suspect gaming accounts with ease.

Unfortunately gaming account status change proved not to be the best way to deal with suspect accounts. First of all, if a Fraud Team blocks a fraudulent customer account right away upon detection, prevents a sign-in, it signals the fraudster that he's been spotted. It thus offers a fraudster an opportunity to instantly make new iterations, find new ways of avoiding detection, learning faster. This kind of petty fraud fighting surely is interesting, like playing a giant computer game with the opponents evolving all the time, or cat and mouse, but so very inefficient. Secondly, very thorough screening and monitoring will reveal possible fraud, but it will create false positives, too: Perfectly good, honest customers might occasionally take the hit. And the worst thing for company reputation and the Customer Service workers is an honest playing customer who might feel unsure what is going to happen and whether they will get their money or not.

4.10 Towards a better user experience

Thinking of usability and customer experience, it would be much better to let the people sign in freely, play – never to let the gaming site reveal that there is anything special going on behind the scenes. The only thing that needs to be controlled is withdrawals and money transfers, because only there can money be lost. Playing is not a problem, because in long run, the house always wins and the fraudsters accounts will become drained by themselves, leaving them no need to contest the Customer Service or Fraud Teams for any money. So, instead of account status change, suspect accounts should be tagged and money transfers suspended until the necessary verifications have been made. A carefully adjusted selection of business rules could be applied to all playing customers to make screening and monitoring less important: For example, an unidentified player should never be able to withdraw in total more than he has deposited in total, an unidentified player should only be allowed to transfer to an external gaming service provider i.e. poker an amount he has deposited using a safe payment method plus the amount he has previously transferred from the same ESP, to name some ideas. Transfers, withdrawals of players with certain payment methods and gaming behavior should be automatically put on hold until a thorough identification and any necessary background checks have been done. How tight the business rules are affects the need of resources available at Customer Service for explanations and Fraud Teams for identification and investigation. Of course delays in withdrawals are not desirable, but they are way easier to explain away as technicalities than blocked accounts.

Communication is very important, too: The Marketing Teams, Customer Service Teams and Fraud Teams should always be aware of any new promotional campaigns well in advance, discuss the implications and constantly keep each other informed about the impact they have on them. And communication must include customers, too: The rules should be simple and transparent, encouraging early, voluntary identification in order not to delay withdrawals processing or other transfers of funds. This way, Customer Service teams will have more time to help the players with happier things, giving a better consumer experience.

And as for the free lunches, they have been discontinued virtually everywhere. Perhaps the continuous fraud attempts had some effect on this. There are greater considerations, however: First of all, an initial deposit should always be required when granting a bonus to make sure the player has suitable payment instruments (and balance) available for playing. Secondly, with huge turnover requirements, huge bonuses can be advertised: A majority of players would rather take a 1000 euro bonus than a 20 euro bonus on top of their 20 euro deposit: The turnover requirement is written in a smaller print, and the operators rather fancy customers who do not calculate probabilities, anyway. The scariest part of the huge bonuses with huge turnover requirements is, however, that the biggest ones available are for slotmachines only. Slotmachines are the crack-cocaine of money gaming; And a certain percentage of population is always very prone to gaming addiction. One can't help suspecting that granting this kind of bonuses would be an intentional, a well-planned strategy for triggering gaming addiction and problem gaming.

5 CONCLUSION

It has been over 10 years since the author first started working in the online money gaming industry. Looking back, one feels a sort of nostalgic about it. Many things have changed: Some truly internationally oriented gaming companies have already changed their focus and offer their services to fewer, even regulated markets with larger volumes in exchange for simpler processes and tools: developing world or economies in transition have brought in few players, the risks in these are high, identification integration is impossible and the culture is often unknown. At the same time, tiny new gaming companies are popping up to fill in the void, but often with limited, safe gaming product categories and payment options; it is possible nowadays to buy such fully working gaming systems with a few hundred thousand euros. In these, the work of fraud teams has been reduced to almost just checking identities and withdrawals.

Nevertheless, one might wonder whether it was then, perhaps, very inefficient, false usability to make tools for early fraud detection, monitor the players' undertakings, getting to know them and their sign-up patterns and gaming behavior -Yes and no: Of course, everything that can, should be automatised, for sooner or later one needs to ask: If you can not afford a technical, automatised implementation, can you afford not to make one? Still, someone should always have an idea of what is going on, what the players are up to. When that someone knows what's going on, it is easier to strive for those automatized technical solutions. The author was working in companies with in-house software development. An open-minded atmosphere and a positive attitude towards fraud analysts designing and prototyping their own tools helped to produce lots of fresh ideas and new tools. Later on, some of these tools would go through the company official release process and become part of the standard.

REFERENCES

FBI. 2007. Online Gaming. Don't Roll the Dice. Consulted 06/06/18.

https://archives.fbi.gov/archives/news/stories/2007/june/gambling_060607

Finanssiala. 2011. TUPAS service description. Consulted 18/02/2018.

http://www.finanssiala.fi/maksujenvalitys/dokumentit/TUPAS_service_description_v23c.pdf

Finanssivalvonta. 2010. Standardi 2.4. Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen.

http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2.4.std5.pdf

Kuustie, H. 2015. Money laundering prevention – From International standards to Finnish banks. Turku University of Applied Sciences.

KRP. 2014. Rahanpesun selvittelykeskuksen vuosikertomus 2014. Consulted 18/02/2018.

https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/28746_Rahanpesun_selvittelykeskuksen_vuosikertomus_2014.pdf?fb1b8f87a9eed488

MGA. 2018. Malta Gaming Authority. Directive X of 2018. Player Protection Directive. Part VIII - Protection of Minors and Vulnerable Persons. 26. (3).

Nya Aland. 2017. Penningtvättåtal mot Paf och förra vd:n. Consulted 18/02/2018.

http://www.nyan.ax/nyheter/atal-mot-paf-och-dess-forra-vd/

Oracle.

http://www.oracle.com/technetwork/oem/uxinsight/realuserexperienceinsight-085193.html. Consulted 22/03/2018

Paysafecard. 2018. Pricing models for online partners. Consulted 18/02/2018.

https://www.paysafecard.com/en/business/online-partner/pricing/

Splunk.

https://www.splunk.com/en_us/products.html. Consulted 22/03/2018

Svenska Dagbladet. 2014. Jimmie Åkesson har spelat för en halv miljon.

https://www.svd.se/jimmie-akesson-har-spelat-for-en-halv-miljon. Consulted 18/02/2018.