Raising Standards in Compliance: Application of artificial intelligence to online gambling data to identify anomalous behaviours

Industry Stakeholder Interview Whitepaper

2nd July 2018

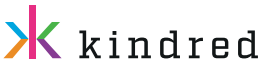
Authors:

Charitos Charitou, Ph.D Candidate at City, University of London (charitos.charitou@city.ac.uk)

Simo Dragicevic, Ph.D Supervisor at City, University of London and CEO, BetBuddy, Playtech Plc (simo.dragicevic@playtech.com)

Professor Artur Garcez, Director of the Research Centre for Machine Learning at City, University of London (a.garcez@city.ac.uk)

Stakeholder Interviews



Alexanda Henderson	Ex-Law Enforcement AML Investigator
Alexander Mangion	Head of Legal and International Relations Section, Financial Intelligence Analysis Unit, Malta
Alfred Zammit	Deputy Director, Financial Intelligence Analysis Unit, Malta
Asaf Greenhouse	Deputy MLRO, Playtech Plc
Claire Wilson	Senior Manager and AML Specialist, Great Britain Gambling Commission
Clive Hawkswood	CEO, Remote Gambling Association
Dominic Micallef	Chief Officer Enforcement, Malta Gaming Authority
George Debrincat	MLRO, Kindred Group
Ingrida Lafzi	Compliance Officer, Playtech Plc
Karl Buhagiar	Head of Legal and Compliance Operations, Kindred Group
Paul Buck	CEO, EPIC Risk Management
Virginie Come	AML Operations Manager, Kindred Group

Introduction

The European Union's 4th Anti-Money Laundering (AML) Directive has increased the pressure on the online gambling industry to ensure it is not used as a vehicle for terrorism finance, money laundering, or for leisure spending from the proceeds of crime (collectively these fall under AML). Until recently, the industry has tackled the identification of crime in online gambling primarily by using knowledge-based systems. Whilst capable of easily embedding regulatory requirements which have focused on simple thresholds, these systems are unable to adapt to new requirements to proactively monitor the activity of millions of online customers and changing behavioural patterns related to criminal activity online.

Whilst improvements have been made, the online gambling industry needs to continue evolving and raising standards in compliance monitoring. In Great Britain, the Gambling Commission has sent a clear message to gambling operators to raise standards in compliance and to place consumers at the heart of their businesses, warning that regulatory breaches could lead to higher financial penalties and even the possibility of license review and revocation. The Great Britain Gambling Commission (the "Gambling Commission") also states that compliance with AML and Counter Terrorism Finance (CFT) starts with a supportive culture at Board and Senior Management level. The Gambling Commission also states that compliance with AML and CFT must be achieved through a culture, at Board and Senior Management level and then throughout its firm, that promotes and effectively embeds compliance with the firm's legal responsibilities in this strategically significant area.

In recent years, the Gambling Commission has begun to take more punitive action against operators for regulatory breaches. For example, 888 Holdings was subject to a record regulatory settlement of £7.8m for failings in social responsibility practices, with one customer having stolen £55,000 from its employer to fund their gambling habits. LadbrokesCoral Group was ordered to pay £2.3m by the Gambling Commission for failing to intervene after two problem gamblers lost £1.3m of stolen money whilst engaged on its online casino. Most recently, William Hill was also subject to a regulatory settlement of £6.2m for failing to protect consumers and to prevent money laundering, and 32Red, now part of Kindred, was given a £2m penalty for failing to identify and terminate problematic behaviour of a single customer relating to gambling addiction and money laundering.

In 2017, Kindred Group, one of the world's largest online gambling groups, entered into a research collaboration with the Research Centre for Machine Learning at City, University of London, and BetBuddy, now part of Playtech Plc. The purpose of the research is to explore the use of Deep Learning and Artificial Intelligence (AI) techniques to strengthen processes to detect suspicious gambling behaviour in relation to AML. The first stage of the research focused on interviewing a variety of industry experts and stakeholders to understand the current state of the industry's approach and capabilities to tackling these issues, specifically looking at where technology could be used to raise standards. The subsequent research phases will be focused on exploring techniques to better monitor and flag suspicious gambling behaviours.

This paper summarises the key discussions taken from the expert and stakeholder interviews, which included experts from national crime agencies, regulators, trade associations, suppliers, and operators. We also provide some technical recommendations for industry and guidance that will inform the next phase of research.

Is Crime in Online Gambling a Major Industry Issue?

Historic Issues in Crime and Gambling

Money Laundering is the world's third largest 'industry', with an estimated $2 trillion laundered every year[1]. If criminals want to profit from crime and avoid prosecution they must find a way to cover the origins of their stolen gains. Thus, every crime that involves stolen money ends with money laundering or spending the proceeds of crime. In the context of this whitepaper, AML covers criminal leisure spend, smurfing, money from stolen goods, and money from drug dealing, for example.

The traditional gambling industry, as a cash-oriented business, has in the past offered plenty of opportunities for criminals to engage in money laundering and in spending the proceeds of crime. In the past there was little in the way of Know Your Customer (KYC) checks in gambling and it arguably was easy to spend and recycle stolen money in physical casinos and other land-based gambling establishments, such as high street bookmakers.

Even though the online gambling industry has required all players to be registered, traditionally KYC checks were non-mandatory for those depositing and gambling with larger amounts of money. The last decade has seen the introduction of new, much more stringent regulations that have required the online industry to become more vigilant. For example, in Great Britain, whilst the Gambling Commission has had in place a sufficient legal framework for all gambling businesses to prevent and detect money laundering and terrorist financing since 2007, it has been gradually increasing in regulations in line with developing evidence. However, as standards began improving, the methods used to process finance from illicit activities also evolved and became more sophisticated.

One method that was consistently mentioned during the stakeholder interviews was a process known as 'smurfing'. Smurfing involves the distribution of cash into a number of smaller transaction amounts to evade threshold requirements and minimise suspicion. This technique was traditionally used in physical casinos with a large degree of success. Whilst there remains a continued risk of 'smurfing' in the online gambling industry, some stakeholders stressed that this is a much lower risk activity compared to leisure spending in online gambling that is funded through the proceeds of crime.

[1] MONEY-LAUNDERING AND GLOBALIZATION
Unodc.org. (2018). *Money-Laundering and Globalization*. [online] Available https://www.unodc.org/unodc/en/money-laundering/globalization.html [Accessed 17 Apr. 2018].

Is Online Gambling an Attractive Avenue for Crime?

The continued increase in regulations centred on preventing criminal spend in online gambling has certainly made it a more difficult channel for money launderers. However, throughout the stakeholder interviews, we heard different opinions, as well as evidence from investigative cases that regulators have dealt with as to whether or not online gambling remains an appealing avenue for criminal spend.

Whilst registered play and enhanced KYC processes have increased surveillance, the only restriction to prevent anyone from opening an online account is age. Cash-based payment methods, such as pre-paid cards, as well as emerging payment methods such as digital currencies, allow customers to deposit money without having to rely on traditional bank accounts (where typically enhanced KYC checks will have been undertaken in a face-to-face manner). As a result, today the source of funds of online gambling customers can remain unknown and difficult to trace. In fact, it was stressed that because there is no face-to-face contact during account opening in online gambling as there is in banking, the KYC process is weaker and potentially open to abuse.

One point that was repeatedly made during the interviews was that history suggests that many criminals enjoy gambling; therefore the AML risks in the gambling industry are higher than in other industries. And whilst many regulated jurisdictions are making progress in tightening systems to make it harder for criminals to launder and spend money, there remain many jurisdictions where standards and regulations remain too loose.

Despite these, some stakeholders expressed the opinion that online gambling today is mature in regulated markets and is not an easy place for criminals to spend and launder money. The increase in security by online operators (i.e. in requesting more information) has made it much harder for criminals to go undetected. Also, the recent high-profile cases of regulatory action against some of the most established and successful online gambling operators in the world shows that there is considerable pressure on the industry to continually tighten checks and to close loop holes. This applies even more so for land-based gambling where unregistered play is possible (i.e. cash-based gambling where the gambler does not hold an account and is not part of loyalty card scheme that tracks their play and spend).

Key Business and Regulatory Challenges in Combatting Crime in Gambling

Criminals Staying One Step Ahead

Criminals were consistently described as sophisticated by stakeholders, in that they have the ability to stay 'under the compliance radar' for long periods of time, making it difficult for compliance departments to track them.

Despite this, it was stressed that this certainly does not apply to all cases, and the cases publicised by the Gambling Commission have concerned obvious examples of high-spending individuals being missed by operators. Evidence from regulatory investigations demonstrates that operators have usually identified high-spending criminals first as VIPs (Very Important Person, typically high spending customers), only then to discover they are leisure spending criminals.

A former gambling addict explained that despite the current checks in place in online gambling, it is still relatively easy to develop strategies using multiple online gambling accounts to remain under their respective compliance controls and checks. The current rules-based systems adopted by most operators for their AML and proceeds of crime monitoring checks were argued to be too rigid, as criminals can quickly adapt to known rules and thresholds. Moreover, criminals are often well educated about the regulations and can use the laws against the operators themselves to help cover their tracks; e.g. data privacy and protection laws. Having said this, it was also stressed that, whilst the General Data Protection Regulations (GDPR) do rightly afford players privacy, retention of information and information requests can be made by law enforcement agencies and the Gambling Commission. These requests would effectively lift the veil on the privacy of criminals if they were asked for in the event of detecting and preventing crime and in the public interest.

Our stakeholders said that it was critical for the industry to do everything it can to keep criminals guessing; in effect 'out-smarting' them through the development of new methods and systems they are unfamiliar with. But to reduce risk and eliminate criminal activity, the industry of today needs more targeted and sophisticated strategies that provide new ways of identifying suspicious and criminal activity. In parallel, it was also stressed that the industry should not decrease focus on correctly and consistently applying the very basic measures within their businesses; something the Gambling Commission has repeatedly failed to see in enforcement casework.

Elevating the Importance of Compliance Across Departments

It was noted by the regulator and other stakeholders that raising standards and protecting the consumer and wider public in the culture of gambling businesses is essential to mitigating the ongoing AML and CFT risks, with Board and senior management leadership viewed as critical to success. Whilst it will take time to accomplish this objective across the industry (notwithstanding that requirements have been in place since 2007 in Great Britain), it was stressed by the Gambling Commission that the industry operates in a regulated market, with applicable laws and regulations with clearly stated compliance requirements that need to be implemented today. Whilst the scope and work of compliance teams is increasing to ensure new regulations are met, our stakeholders explained that there are many challenges to overcome. It was also stressed that despite these resourcing challenges, the Boards and Senior Management have to effectively resource the MLRO/Nominated Officer and in the training of employees, which are critical in becoming more effective.

- Convincing marketing teams to follow a more strategic approach on AML and responsible gambling issues – Whilst Customer Relationship Management (CRM) optimisation (e.g. profitability, customer acquisition and retention) will remain as the main priority, operators should become more customer protection-oriented. This requires revenue generating teams to see the value in having class-leading compliance capabilities, and to understand the associated investments and commitments required. It was stressed that industry must embed compliance throughout the business, including in the marketing teams. AML offences apply to individuals, and gambling staff could be leaving themselves open to committing crimes by permitting the proceeds of crime to flow through their business. It was also stressed that a compliance rich commercial team can be a commercial advantage in preventing regulatory action.

- Changing the mind-set of staff – Some casino employees, such as croupiers, have been in the industry for many years and may have learned to work in a certain way; e.g. not to flag a suspicious customer who tips them (notwithstanding in Great Britain where the Gambling Commission's Licensing Conditions and Codes of Practice requires casinos to operate a tronc tipping system, where all tips are pooled and distributed amongst the employees concerned); a clear but often understandable conflict of interest, given salaries in these jobs are comparatively low. Getting staff to adjust to regulatory changes is therefore difficult. However, the risks regarding permitting crimes outlined above apply here too.

- **Requesting information from the customers** – For operators it is challenging to convince their customers why extra information about them is needed. Customers will often question requests to validate Source of Funds (SOF) and Source of Wealth (SOW) and may see such requests as an invasion of privacy and go to competitors who may not be applying as stringent checks, in effect rewarding less compliant operators with valuable and legitimate customers. Whilst a genuine concern raised by industry, the Gambling Commission stressed it expected all operators to comply with this requirement. Some argued that, in effect, this is unfairly penalising those operators investing in compliance. It was also noted that there have been cases where people are warned by authorities (e.g. the police) against providing personal details to companies, which can make achieving compliance SOF and SOW checks challenging.

  A counter-argument to this was that customers already have to share personal information when opening an account or wish to receive marketing and rewards, and this is simply a request for more information – and that operators should be curious as to when customers are not prepared to offer the information. In addition, it was stressed that SOF and SOW checks also involve using information not provided by the customer. It was highlighted that the industry needs to re-educate its customers that, if they wish to gamble in a certain way or over certain monetary thresholds, they will be asked questions and asked to prove things. This is very common practice in other industries such as retail banking or high value goods purchase. Ultimately, it is a legal requirement (e.g. to enable cross-checking of sanctions databases in the regulated casino sector) and licensees leave themselves open to offences if they fail to do this.

Limited Feedback on Cases

For every suspicious incident observed operators are obligated to submit a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) (including Defence Against Money Laundering, or DAML reporting in Great Britain too), which is typically passed on to the local crime agency to review; e.g. the National Crime Agency (NCA) in Great Britain and Financial Intelligence Analysis Unit (FIAU) in Malta.

A major limitation of the process today is that crime agencies provide limited feedback to the operators, including both specific feedback on individual SARs as well as feedback on the system generally. There are some exceptions. In Malta for example, the FIAU issues an annual report in which they make public the analysis of the SARs that they have received. The NCA also produces an annual analysis of the SARs submitted to them.

Moreover, every operator receives a receipt and a score regarding the quality of their submitted reports. Finally, the FIAU informs the operators whether the incident is investigated or not. This not the case with intelligence agencies in other jurisdictions, although some of these practices are likely to be increasingly adopted (e.g. in Great Britain). All stakeholders saw an opportunity for the authorities and industry to work together to improve the process, primarily to enable operators to share data and learn from previous experiences. However, currently no legal gateway exists that enables law enforcement bodies or regulators to share

information or intelligence about other businesses, with the lack of process here a barrier.

Our stakeholders explained that the main reasons for limited feedback on cases is that thousands of reports are submitted every day, which have to be reviewed and investigated. The agencies therefore struggle to manage the increasing volume of cases. In addition, agencies need to be very cautious given the possibility that criminals have connections working inside gambling operators which could compromise their investigations, making data sharing and feedback a sensitive area.

This absence of feedback, whilst not increasing the accountability and responsibility for operators, makes the process more challenging for them. It was stressed that, because the regulator or agency cannot take the responsibility to advise on whether or not to close a customer account due to a SAR or STR being raised, compliance teams have to take critical decisions about whether to continue accepting money from these customers. These teams also have to make these decisions in the knowledge that commercial teams often have the opposite business objectives in principle (although the Gambling Commission stated it disagreed with any perceived conflicting business objectives). In cases where evidence is sparse, the industry has some very challenging decisions to make, as legitimate customers could be turned away and driven to competitors with less robust monitoring in place, as outlined earlier.

Today crime agencies have to deal with greater volumes of STRs and SARs, as pressure increases on operators to do more to flag suspicious behaviours. Given this, stakeholders acknowledge it would be beneficial for all parties involved if better communications could be established between operators and crime agencies.

Another area flagged as having potential for improvement was the process of submitting STRs, SARs and DAML. Currently it is a highly manual and time-consuming process, with different formats and standards adopted by different jurisdictions. Developing a single technical submission format (e.g. a consistent API or XML standard) for STRs and SARs would be beneficial and save costs that could be re-invested in improving detection capabilities.

Key Technical and Legal Challenges in Combatting Crime in Gambling

Limitations of Rules-Based Systems

Whilst regulatory investigations have highlighted cases of sub-optimal industry standards, it was stressed that a risk-based approach is being increasingly adopted by the industry to ensure that measures to avoid or mitigate money laundering, terrorist financing and proceeds of crime are proportionate to the risks identified, ensuring resources can be allocated in the most efficient way.

As discussed earlier, the increased monitoring expectations are posing significant operational challenges for operators, with some stakeholders stating that compliance costs have increased significantly and that increasing coverage using the current systems and tools could easily double compliance team sizes. A counter argument was that compliance costs have increased due to sustained

underfunding in this area for a long period of time. This has led to poor standards and subsequent regulatory enforcements cases, which has required licensees to now invest heavily to bring their basic standards up to an acceptable level.

Having more effective systems in place to analyse and process all of these risks is therefore becoming increasingly strategically important. Until now, systems with specific rules and thresholds have been integrated by operators to monitor their business, often by adapting and evolving existing back office systems that undertake core gambling processes (e.g. registration, player wallet, payments etc.) However, such rules-based systems have disadvantages:

- **Ongoing maintenance:** Adding new knowledge to the system to solve other problems could lead to contradictions with old rules.
- **Ineffective:** Rules-based systems are not effective at widening the net of analysis; rather they focus on absolutes and often extremes.
- **Easy to understand:** Criminals could very easily stay undetected if they know a system's rules. They could adjust their approach and use different methods to stay unnoticed while the system's rules remain static, rather than dynamic.

It was stressed that some of the larger operators have improved their procedures and checks, but largely it was felt the industry is relying on very similar processes and thresholds. It was stressed that more investment is vital for the industry to demonstrate it is approaching this issue in a smarter way. A consistent theme from stakeholders was that smaller and medium-sized operators would find it challenging to find resources to implement 'step changes' in capability, as the majority of spend is focused on competing with larger brands (i.e. increasing customer acquisition and retention costs).

Improving Source of Fund (SOF) Checks

Over the years, verification checks have become a regulatory requirement for the industry. The need to 'know your customer' has been proved to be essential for the industry to protect the players from identity theft and operators are required to check both SOF and SOW when necessary. Moving forwards, information regarding SOF of customers is likely to be an increased requirement to verify the affordability of certain customers from a crime and responsible gambling perspective. This is an area the Gambling Commission is currently consulting on[2].

Some stakeholders felt that the gambling industry needs to concentrate more efforts in the verification process and with SOF checks. For example, operators should be implementing systems to identify patterns that uncover any suspicious behaviours and conflicted evidence from larger spenders,

[2] GAMBLING COMMISSION MAKES ONLINE GAMBLING SAFER

Gamblingcommission.gov.uk. (2018). Gambling Commission makes online gambling safer. [online] Available at: http://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/Gambling-Commission-makes-online-gambling-safer.aspx [Accessed 17 Apr. 2018].

where typically, more risk associated with criminal spend has been evidenced in the past – e.g. an unemployed customer is spending a large amount of money, customers are not withdrawing money, customers are refusing hospitality, customers live in an expensive house with a low paid job etc. It was noted that human oversight plays an important role here, through the application of observation and common sense. However, the ability to apply human observation and reasoning to all gambling activity was stressed as operationally challenging; hence the need for systems to support humans.

It was also noted that the process to complete SOF checks is largely administrative and implemented without much thought to the end customer experience. Customers are becoming increasingly savvy about forthcoming regulations, such as the General Data Protection Regulations (GDPR); therefore an opportunity exists to educate the customers and build trust via any SOF processes if well thought through and implemented.

Lack of Data Sharing

Whilst the volume of customer data is growing faster than ever, data protection laws are becoming increasingly tighter. Data that is combined and shared often has the potential to be much more useful than in isolation. For example, GAMSTOP will enable some limited sharing of data on self-exclusions to enable operators to check whether a player has voluntarily registered on the scheme. This will improve customer protection standards in online gambling in Great Britain, having already done so in other jurisdictions such as Spain, France and Denmark.

Even though data sharing is a very challenging legal task, stakeholders stressed some ideas are worth pursuing, such as a central database of originator details for access by Money Laundering Reporting Officers (MLROs). All the flagged and reported cases could be stored in a central and secure database, to which all operator MLROs would have access, to enhance ongoing monitoring in their own operations. However, it was noted that this issue would pose complications for whoever becomes the data controller for the shared information.

However, sharing personal information about customers' suspicious gambling behaviours is not something that is expected to materialise soon according to most stakeholders interviewed. Data protection laws, such as GDPR, protect customers and do not allow for operators to easily exchange personal data. Most stakeholders felt that this was a problem that was very difficult to resolve in the short term.

Despite the legal challenges, various discussions are ongoing in the industry regarding data sharing, as the benefits are acknowledged to be potentially significant. And whilst operators currently cannot share information about their players, they could better use the data that is available in the public domain to build the players' profiles. However, recent cases such as that with Facebook and Cambridge Analytica[3] may make the use of social media customer data a legally thorny issue to tackle.

[3] FACEBOOK CAMBRIDGE ANALYTICA SCANDAL: HERE'S WHAT HAPPENED

Fortune. (2018). Facebook Cambridge Analytica Scandal: Here's What Happened. [online] Available at: http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/ [Accessed 17 Apr. 2018].

Some organisations are trying to look at tackling this issue in different ways; e.g. the introduction of an AML questionnaire, which will enable the operator to learn more about the customer, such as how much they want to spend and what they want from their gambling experiences. This could also help to improve ongoing responsible gambling check and processes.

Convergence of Land and Online

Whilst land-based operators have the advantage of been able to talk and visibly observe their customers, they have difficulty linking information to a person's online account, when a customer plays in a retail outlet, but also deposits monies over the counter into their wallet. If a customer is playing in a retail shop and then wishes to deposit or withdraw from their e-wallet, they should be asked for their name and passcode so that they are identifiable.

That consumer can then play online with that money, either in a regulated or non-regulated sector. The movement of such monies from an offline to an online environment, and then from non-regulated to regulated, is a challenge for the industry and considered an area where operators need to raise standards in AML and CTF. The evolution of single customer wallets for both land and online gambling will improve operators' ability to have a single view of all player activity.

Industry Approaches to Tackling Crime in Gambling

Industry Collaboration Across Shared Issues

Collaboration between stakeholders is seen as a key factor in raising standards. Trade associations and regulators work hard to maintain high standards in the industry and developing collaborative working relationship through organisations such as GAMLG (Gambling Anti-Money Laundering Group) is essential for facing shared problems. For example, the Gambling Commission supports such collaborations with regular workshops and publishing guidance about emerging criminal typologies and encourages collaboration cross all sectors; i.e. non-remote and remote licensees sharing learning and ideas. It also publishes specific guidance to both the regulated and non-regulated sector for AML and CTF purposes to comply with statutory requirements of regulations.

Also, GAMLG has provided guidance[4] on a range of Customer, Product, Payment and Employee Risk areas that should be assessed; e.g. withdrawing without play. These are essential for the small operators who often struggle to be able to spend as much as larger operators on compliance research and development. However, it was stressed that such guidance also enables criminals to adapt behaviours to try to avoid detection, requiring the industry to continually re-assess and evaluate how to track suspicious play.

[4]GAMLG
Rga.eu.com. (2018). [online] Available at: https://www.rga.eu.com/wp-content/uploads/GAMLG-AML-Risk-Assessment.pdf [Accessed 17 Apr. 2018].

In response, it was also noted that the mitigation to this risk is that GAMLG also produces work which, for exactly this reason, is not in the public domain; i.e. full industry risk-assessment for internal use only to avoid providing criminals with a shopping list of industry vulnerabilities.

It was noted that the industry could also invest in new relations, for example with the banking industry, to learn how they have managed compliance risks in the past.

Simple

Complex

Domain	Type	Description
1. Deposit Threshold	Absolute	Flags whether a deposit exceeds an absolute threshold. Configurable and also looks at thresholds checks per day / week / month. Multiple thresholds could be added that randomly change
2. Spend Threshold	Absolute	Flags whether spend exceeds an absolute threshold. Configurable and also looks at thresholds checks per day / week / month. Multiple thresholds could be added that randomly change
3. Near Thresholds	Absolute	Flags whether a player reaches within a set % of the limit/threshold for Deposit and Spend.
4. Deposit/Spend to Withdrawal Ratio	Ratio	Spots players who have a very low withdrawal ratio compared with a comparatively high amount of gambling activity
5. Deposit Threshold Ratio	Ratio	Spots players who consistently deposit a little below a regulatory threshold to get round being flagged.
6. Spend Threshold Ratio	Ratio	Spots players who consistently spend a little below a regulatory threshold to get round being flagged.
7. Suspicious Play Check	Machine Learning	Based on patterns of known money launderers, however predicting very rare events is hard and very little training data exists (i.e., 'ground truth')
8. Anomaly Check (Player)	Machine Learning	Spot anomalies based on what is considered normal e.g., deposit, spend, loss, etc.
9. Anomaly Check (Branch, Game, Game Type, etc.,)	Machine Learning	Spot anomalies based on what is considered normal in a branch, game, game type, time of day, etc.
10. Affordability Check	Machine Learning	Uses internal and external data (e.g., social media, credit) to derive affordability thresholds for each player and check activity v. what is expected. Complexity lies in navigating cost and privacy issues with accessing external data.

New behaviours can be analysed and methods tested to potentially improve monitoring

In Malta, the MGA works very closely with the operators to ensure regulations are being followed. To serve this purpose they have started to supervise operators and oversee how well current policies are applied. At the same time FIAU in Malta aims to provide as much feedback as possible to the gambling operators, starting with quality scores on the submitted SARs; something the National Crime Agency (NCA) is also looking to implement.

Investment in New Technologies

A major reason for investing in new technology to monitor for suspicious behaviours is the increasingly high volume of transactions in online gambling. The use of new technologies and more intelligent systems is likely to become a requirement for operators in order to meet future regulatory obligations. In fact, some stakeholders suggested that the only way to meet obligations in future would be through using techniques related to Artificial Intelligence (AI).

AI can help to assess patterns, trends and anomalies, and even correlate networks IP addresses with crimes. The alternative to investing in new technologies is either i) scale-up the size of AML and CTF teams (i.e. significantly higher costs) or ii) to limit the scope of ongoing monitoring to what current team sizes can manage (i.e.

significantly increased risks). Another way of defining investment needs was to assess the regulatory risk of losing a licence and to invest what is necessary to prevent that.

Whilst investment in technology was supported by all, it was stressed also that concentrating on Board and senior management buy-in, culture and getting basic requirements right was also critical, and would arguably require less investment.

Combining Analysis of Proceeds of Crime Alongside Problem Gambling

Some operators have suggested that up to 80% of the suspicious cases they receive are assessed for both Responsible Gambling (RG) and proceeds of crime. This link between RG and proceeds of crime cases is described in BDO's report[5] that shows that problematic gambling is the biggest reason for frauds involving spend of over £55,000. This is further supported by recent enforcement action cases in Great Britain. Whilst this link between cases was well known with all of the operators interviewed, stakeholders felt that closer collaboration between the operator RG and AML teams will continue to be required in future.

Summary of Key Technical Recommendations

Whilst many areas for improvement were identified during the interviews, we have limited the focus of this paper to technical recommendations, of which those related to operators will provide the focus for subsequent technical research;

For Crime Agencies

- Develop a single format or technical protocol for submitting STRs, SARs and DAML across jurisdictions that enables operators to submit cases using a consistent system, whilst also providing feedback on submission quality. This will i) enable industry to save money on the increasing manual efforts and costs to submit returns and re-invest in improving systems, and therefore the quality of submissions; and ii) subsequently reduce the load on the agencies by reducing the number of poorer quality cases.

For Regulators

- Continue exploring opportunities to develop a single central database for customers flagged for suspicious gambling activity, to enable enhanced monitoring of flagged customers across industry. Combining data can have a significant impact on improving compliance processes in the industry, thus raising standards (although it was stressed in GB, for example, that the legal responsibility for this issue sits with the Information Commissioner's Office).

[5]BDO FRAUDTRACK 2018
Bdo.co.uk. (2018). BDO FraudTrack 2018. [online] Available at: https://www.bdo.co.uk/en-gb/insights/advisory/forensic-services/bdo-fraudtrack [Accessed 17 Apr. 2018].

For Online Gambling Operators

- For threshold checks, explore the addition of both more threshold[6] levels above the current regulatory requirements and also the introduction of variable elements in the process. A threshold randomisation algorithm could be implemented to modify levels below regulatory standards, keeping criminals unaware of when a transaction could be flagged. However, it was noted that a system that relies solely on thresholds would not be particularly effective at identifying potential money laundering activity.

- Develop more sophisticated and cost-efficient methods to improve ongoing monitoring. This entails building techniques that analyse player behaviour below the minimum threshold levels required by regulators, whilst not relying on increased staff numbers to broaden monitoring scope.

- Use data to develop more sophisticated behavioural checks and customer affordability segments to support enhanced source of funds checks throughout the customer lifecycle for higher spenders, and not just at specific points such as regulatory threshold breaches (e.g. a customer depositing over €2K within a 24-hour period).

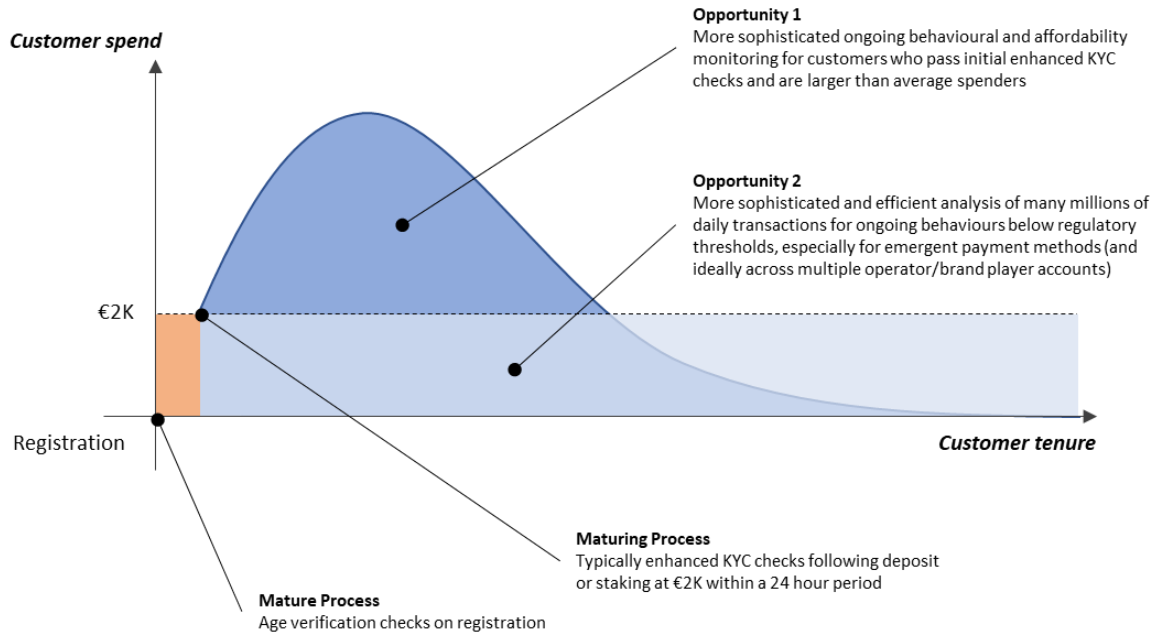
- Invest in modernising and simplifying KYC and SOF processes, using it as an opportunity to build a closer customer relationship and to build trust in the brand, and not view it as an administrative or 'check box' compliance process.

- It was noted that external expert review to ensure systems remain up-to-date should be considered. Whilst this is a matter for operators to consider, some regulators have observed this has reaped benefits.

Next Phase of the Research

The findings from the stakeholder interviews suggest that whilst the current systems and processes on registration and at regulatory thresholds are reasonably robust, more focus needs to be given to the ongoing monitoring of the customers' behaviours. This suggests that typically only a small percentage of the customer behaviours are subject to detailed and ongoing customer analysis from an AML and proceeds of crime perspective;

[6] There is no de minimus threshold for criminal spend, there is a 2000 euros transactions threshold where CDD must be completed, however points before the 2000 euro threshold can trigger CDD such as forming a business relationship or forming a suspicion or gaining knowledge of money laundering. These are the only legally applicable thresholds for casino operators. I think you should be arguing for casino operators to be monetarily below the current thresholds and above regulatory requirements. For the non-regulated gambling businesses a risk-based approach should be demonstrated through their risk assessment as to how they agree a monetary threshold.



Opportunities to improve ongoing monitoring

Opportunity 1 is centred on better monitoring of higher spenders who, evidence suggests, are more likely to be criminals, from both a behavioural pattern and SOF assessment. Opportunity 2 is focused on those criminals who keep activity below static regulatory thresholds (e.g. if a customer deposits over €2K within a 24-hour period). This second opportunity would ideally benefit from the sharing of operator data on suspicious behaviours. However, this is unlikely to materialise in the short-term, so will remain a very difficult technical challenge. One area to focus on here will be the use of new digital currency or cash-based payment methods; e.g. pre-paid cards. For larger operators who manage multiple brands, combining data across multiple accounts may reap benefits and could be considered.

The objective of this research is thus: the development of an adaptive, real-time monitoring system that could be facilitated by self-learning models. The next step to achieve that target starts with assessment of the quality of the operator's data. Given that operators receive limited feedback from crime agencies as to whether SARs or STRs lead to criminal investigations (note that operators submitting DAML receive feedback in line with the moratorium period), the number of labelled cases for known criminals will be very limited. Thus, implementing supervised models, which can be used to predict rare events, but which typically require a reasonably large number of historical cases (i.e. several hundred), may be impossible. Due to the unique constraints of real-time applications, applying machine learning could be challenging. Anomaly detection in streaming applications is particularly challenging; operating in an unsupervised, automated fashion is often a necessity. The models that will be developed should continually learn and evolve the behaviour profile of each player and their respective categories. Until now, AML and CTF checks mostly are triggered when the players deposit above a specific threshold level. However, anomalies do occur below that level, which is something the new framework must detect. A research question therefore is to what extent it is possible to detect meaningful types of

anomaly in the gambling sphere using unsupervised learning. This research is in its infancy.

Anomaly detection in time-series, however, is a heavily researched area. Over the years different solutions have been proposed to solve the problem. A method which had good results in detecting anomalies in streaming data is the online sequence memory algorithm called Hierarchical Temporal Memory (HTM). Moreover, Long-Short-Term-Memory (LSTM) networks, a type of recurrent neural network (RNN), have proved to be very effective time series modellers and anomaly detectors for sequential and temporal data. LSTMs have become the deep learning models of choice because of their ability to recall long-range patterns. Similar methods will be investigated and applied during the next phase of this project.

Domain	Type of Machine Learning	Proposed Machine Learning Techniques
7. Suspicious Play Check	Supervised Learning	Random Forests, Bayesian Networks, Multi-Layer- Perceptron
8. Anomaly Check (Player)	Unsupervised Learning	Hierarchical-Temporal Memory (HTM), Long Short-Term-Memory (LSTM), Hidden Markov Models (HMM)
9. Anomaly Check (Branch, Game, Game Type, etc.,)	Unsupervised Learning	Hierarchical-Temporal Memory (HTM), Long Short-Term-Memory (LSTM), Hidden Markov Models (HMM)
10. Affordability Check	Supervised Learning	Random Forests, Bayesian Networks, Multi-Layer- Perceptron

Phase 2 will focus on the most technically challenging opportunities

Other directions of research can be more related to the theoretical underpinning of the models; for example, enhancing the interpretability of the deep neural network models to be developed. In addition, analysing data referring to a single session of play and backpropagation through time may be worth exploring further, as well as the latest proposals in the area of human-like computing, including one-shot and zero-shot learning. The next phase of the research will seek to report progress on these technical issues with the use of real data already kindly provided by Kindred.


kindred


CITY
UNIVERSITY OF LONDON
EST 1894


BetBuddy
a Playtech company