7 Betting (non-remote)

Scale and size of the sector

7.1 The non-remote betting sector has three main subsections; off-course[26], on-course[27] and pool betting. The non-remote sector accounts for approximately 25% of total Gross Gaming Yield (GGY)[28] for gambling in Britain, amounting to £3,201m, and employed 52,566 individuals as of 30 September 2015.

7.2 As of March 2016 there were 259 operators licensed for off-course[29] activity who occupied 8,809 shops. The GB non-remote betting sector is dominated by four operators, which collectively account for 87% of all betting shops. The average total quantity[30] of gaming machines in GB betting shops amounted to 34,807 in the current reporting period and accounted for 56% of total betting shop GGY.

7.3 In the same period there were 546 operators licensed for on-course[31] activity.[32] The largest percentage of GGY from on-course betting between the period October 2014 and September 2015 was on horse racing.

7.4 As of March 2016 there were 26 pool betting licensees. Pool betting includes horse racing, dog racing, football, other sports pools, and 'fantasy football' type competitions. The largest percentage of GGY from pool betting was on horse racing.

7.5 Within the non-remote betting sector the customer base is varied and often customers remain anonymous to the operator (and may be given a *nom de plume*)[33]. The variety of products and high liquidity are key factors which contribute to the exposure of this sector to money laundering.

7.6 The betting industry is not currently regulated under the Money Laundering Regulations nonetheless it needs to comply with the licence conditions and code of practice (LCCP) and POCA, which includes an obligation to report known or suspected money laundering activity. All gambling operators are required to submit suspicious activity reports (SARs) to the UK Financial Intelligence Unit (UKFIU) if they have knowledge or suspicion that a person is engaged in money laundering.

Sector summary

Non-remote betting	Overall rating
	Higher

7.7 The non-remote betting sector as a whole has been assessed as having a risk rating of higher relative to the other gambling sectors. Compliance activity has demonstrated that the off-course non-remote betting sector is failing to meet their anti-money laundering obligations.

[26] The place where the bet is lodged, if it is not physically made at the event. Premises based betting operators may be referred to as off-course bookmakers.

[27] The place where the event takes place. Betting commonly takes place at horse and dog racecourses as well as football, cricket and other sporting events. On-site betting operators may be referred to as on-course bookmakers.

[28] Gross gaming yield (GGY) the amount retained by operators after the payment of winnings but before the deduction of the costs of the operation

[29] Non-remote general betting standard licence

[30] Gaming machine numbers fluctuate during the year and as such operators are required to provide their average number of machines.

[31] Non-remote general betting limited licence

[32] Gambling Commission Industry Statistics

[33] A system operated by the betting sector through which an anonymous customer staking above a certain threshold is given a name often of the operators choosing (the customer's name where known or a descriptor where not) which helps to identify and monitor the customer's activity on repeat visits.

7.8 Common themes emerge in the off-course part of the industry around appropriately assessing customer risk by obtaining adequate information around a customer's source of funds and wealth, failing to respond appropriately to suspicions of money laundering, ensuring effective risk-sensitive policies and procedures were in place to identify money laundering were implemented and failing to manage the money laundering risk, ensuring information sources are effective, and are acted upon.

7.9 The ability of the non-remote betting sector to effectively apply the requirements of the legislation has been called into question. Operators have failed in their ability to apply the requirements to their policies, effectively implement such policies into processes and furthermore assure their processes are effective and continue to be effective. This demonstrates there are failings in the overall control framework put in place by operators.

7.10 Ineffective controls and risk management within the sector increases the likelihood of money laundering to occur. The vulnerabilities relating to licensing and integrity, customers, products and means of payment all have an increased probability of being exploited where the sectors controls are not robust. These overall failures across the sector are taken into account when assessing the likelihood of the individual vulnerabilities being exploited.

Money laundering vulnerabilities associated with the betting sector

7.11 The highest rated vulnerabilities within each category are displayed below. Please note that some of the vulnerabilities only apply to the off-course sector and do not apply to on-course.

Assessment of licensing and integrity vulnerabilities in the non-remote betting sector

Vulnerability
The licensing and integrity vulnerabilities in the non-remote betting sector are:

- betting operations acquired by organised criminals as a means to launder criminally derived funds
- betting employees acting in collusion with criminals to launder criminally derived funds

The potential for betting operations being run by organised criminals is also identified within the UK national risk assessment of money laundering and terrorist financing. Furthermore, FATF[34] recognise employees being complicit in money laundering as a risk within their most recent gaming sector review.

Controls
The Commission mitigates the risk of gambling operations being run by organised crime. The Commission assesses new licence applications (including for personal licences), and current licensees, on a range of factors to ensure the licensee is suitable and the activities they carry out are conducted in a way which minimises the risks to the licensing objectives. The Commission has robust and independently assured controls to mitigate this vulnerability being exploited.

[34] Financial Action Task Force

Although the Commission has a role in licensing individuals in qualifying positions it is the primary responsibility of the operators to limit any risks of employee collusion. In instances where there are concerns over the integrity of a staff member, operators will act appropriately to investigate and take action where necessary. Effective training and monitoring of customers and transactions mitigates some of the risk associated with this vulnerability.[35]

Consequence

The vulnerability relating to licensing risk in terms of betting operations run by organised criminals has materialised to the extent that attempts appear to have been made by organised criminals to acquire gambling businesses as a means to launder criminal proceeds. However, as mentioned previously the Commission's controls have been robust and any attempt by organised criminals to do so appears to have been prevented to date.

The vulnerability of non-remote betting operations run by organised criminals as a means to launder criminally derived funds received the rating of medium-to-higher as the Commission recognises the high impact, but medium likelihood of occurrence.

Concerning the vulnerability relating to betting employees acting in collusion with organised criminals to launder criminally derived funds, the integrity of both controllers and staff employed within this sector have at times been called into question. Properly applied controls by operators can mitigate the risk of employee collusion.

This vulnerability received a rating of medium-to-higher, recognising the high impact but medium likelihood of occurrence.

Assessment of customer vulnerabilities in the non-remote betting sector

Vulnerability

Those customer vulnerabilities assessed within the non-remote betting sector are as follows:

anonymous customers

false documentation used to bypass controls in order to launder criminally derived funds (off-course only)

accessibility to multiple premises/operators (off-course only)

Accessibility to multiple premises/operators and anonymous customers received a rating of higher. False documentation used to bypass controls received a rating of medium.

Controls

All operators must comply with POCA, the LCCP[36] and in respect of these take into account the Commission's advice on POCA as detailed under ordinary code provision 2.1.2. Non-remote betting operators should therefore take a proportionate risk-based approach to AML.

Within the larger off-course operators the controls in place to mitigate the vulnerabilities largely rely on employee awareness and automatic financial triggers on products to alert them to the potential of money laundering.

[35] A new version of the licensing conditions and codes of practice (LCCP) comes into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

[36] A new version of the licensing conditions and codes of practice (LCCP) comes into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering. For example, licence condition 5.1 – cash and cash equivalents, payment methods and services, new licence condition 12 - anti-money laundering and new ordinary code provision 7 – gambling licensees' staff. These conditions will further assist in mitigating the risk of money laundering in gambling once they come into force.

The use of CCTV and employee interaction helps operators build profiles of customers. Betting operators largely use *nom de plume* systems to monitor customers of interest. Larger operators have central operations and dedicated money laundering teams who monitor patterns of spend in near real time, undertake 'know your customer' checks to identify high risk customers and check the validity of documents provided by a customer.

Smaller operators and independent bookmaker controls also largely involve staff awareness of their customers and the nature of their business mitigating much of the risk for example, in terms of footfall, passing trade and size of bets. There is, however, often little continual formal monitoring of customers which can be evidenced by them.

As many of the pool betting licensees have a general betting standard (GBS) licence as well controls within the sector are akin to those in the non-remote off-course part of the sector.

On-course bookmakers record their racecourse business electronically using specialised computer software. The licence holder or employee will usually be accompanied by a clerk who will log the bets made by customers after bets are verbally accepted from cash and account based bettors. These records are occasionally monitored for fraudulent activity. Beyond this, there is little by means of direct AML controls carried out by on-course operators, however, the nature of the on-course environment, for example, the risk appetite of the operators and therefore the size of bets could be considered to mitigate much of the risk of money laundering within this area. Furthermore, the transient nature of customers attending on-course events, and the limited number of on-course betting events taking place on any given day means there are few ongoing customer relationships.

Additionally all gambling sectors[37] whether they fall into the regulated sector for money laundering or not, must complete age verification checks. The Commission, under its LCCP, considers acceptable forms of identity documents to include: any identification carrying the PASS logo (for example Citizencard or Validate), a military identification card, a driving licence (including provisional licence) with photocard or a passport.

Controls concerning accessibility to multiple non-remote betting operators/premises are largely dependent on the individual operator. AML teams from larger operators within non-remote off-course market are increasingly communicating with one another regarding customers of concern.

Consequences

The Commission has evidence that the controls within the non-remote betting sector are not effective enough to mitigate the risk of money laundering. Although it is apparent that some operators are better than others at identifying and mitigating risks. The reporting and detection of suspicious transactions in the non-remote betting sector is often frustrated by the ability of a customer to remain anonymous.

Anonymity is internationally recognised as being an enabler of money laundering. This factor, together with the number of operators a customer has access to, acts to compound the vulnerabilities of money laundering across this sector. The Commission has evidence of money laundering occurring relating to these vulnerabilities.

FATF and the European Commission recognise identity theft as "an increasing trend." It is possible for customers to use false documentation, for example to disguise their identity, to avoid being identified as a high risk customer within the gambling industry.

[37] With the minor exception of certain FECs.

It is becoming increasingly difficult to detect those customers who use false documentation, given the number of sophisticated techniques criminals now employ and the broad range of nationalities the industry attracts.

Anonymity and accessibility to multiple premises/operators were assessed as being higher risk due to the likelihood of occurrence and vulnerability relative to other sectors. False documentation received a rating of medium due to the lower likelihood of occurrence.

Assessment of product vulnerabilities in the betting sector

Vulnerability

The primary product vulnerability assessed within the betting sector is:

Gaming machines, B2 (also known as FOBTs) to launder funds.

This vulnerability is aggravated by the ability to stay anonymous in the sector and the accessibility to multiple premises. The permitted stake levels and game returns also make the use of B2 gaming machines attractive to a money launder.

This vulnerability received a rating of higher and only applies to off-course betting.

Controls

Non-remote betting operators must comply with POCA and have suitable policies and procedures in respect of the Proceeds of Crime as prescribed under the LCCP[38] ordinary code 2.1.2, and for staff to be trained in this area.

TITO in relation to FOBTs can, if appropriately set up, offer a money laundering control rather than a risk. This is because they have the ability, when used in conjunction with CCTV, to provide an audit trail. TITO also offers the opportunity to identify suspicious activity (including insertion of large amounts of money with little or no play, and subsequent presentation and redemption of the ticket value over the counter) using data derived from play. Employee awareness within the betting premises is another factor that mitigates the risk of money laundering.

Monitoring of machine play and automatic alerts and triggers further provide the opportunity for staff intervention and can prompt scrutiny away from shop level within larger operators.

The introduction of a £50 stake requirement[39] provides additional protection, although it has been recognised that most transactions sit below this threshold and the use of account based play remains voluntary. The main control for gaming machines at present is via automated alerts or triggers, and through customer loyalty cards (where a player has signed up for the facility) for which there is no standard approach.

[38] A new version of the licensing conditions and codes of practice (LCCP) comes into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering. For example, licence condition 5.1 – cash and cash equivalents, payment methods and services, new licence condition 12 - anti-money laundering and new ordinary code provision 7 – gambling licensees' staff. These conditions will further assist in mitigating the risk of money laundering in gambling once they come into force.

[39] Customers accessing higher stakes (over £50) are now required to use account-based play or load cash/pay by debit card over the counter. Requiring better interaction between customer and operator for those engaged in high stake play improves opportunities for more effective provision of information and interventions. Source: Gambling protections and controls, DCMS, April 2014.

Consequences

The Commission considers B2 machines, sometimes referred to as FOBTs,[40] to pose the greatest product risk in the betting sector, due to the number and availability of such machines and evidence indicating money laundering is taking place, albeit it is mostly criminal spend. The product vulnerabilities are compounded by the ability for customers to remain anonymous in the betting sector.

Specifically, money laundering through FOBTs with TITO technology appears to be a common theme, although over the counter betting features too. In cases identified by the Commission, the customers were largely monitored (under the *nom de plume*) due to spend levels, but little or no customer due diligence was carried out.

The vulnerability of gaming machines, B2 (FOBTs) received the rating of higher due to being assessed as being likely to occur and having a higher impact relative to other gambling sectors.

Assessment of means of payment vulnerabilities in the non-remote betting sector

Vulnerability

The primary means of payment vulnerabilities for the non-remote betting sector are: cash transactions.

Cash is internationally recognised as being attractive for money launderers and terrorist financers because of its anonymity, being difficult to trace and it is easily transferrable. The UK National Risk Assessment (NRA), for example, highlights the use of cash as being high risk. The vulnerability associated with cash transactions includes, foreign currency, Scottish and Irish notes and fraudulent notes and coins.

Cash transactions within the non-remote betting sector received a rating of higher.

Controls

All sectors must comply with POCA and the operating licence as stipulated by the LCCP[41]. In particular, ordinary code provision 2.1 – anti-money laundering and licence condition 5.1.1 – cash handling.

While in the betting sector it is possible to remain anonymous when conducting cash transactions, betting operators will monitor commercially high risk customers by flagging activity under their name or assigning them a *nom de plume* where the customer's name is unknown, particularly with larger betting operators. The use of CCTV and employee interaction helps operators build profiles of customers. Controls around smaller betting operators and independents largely rely on staff awareness of customers, and the nature of their business for example, the footfall and size of bets limits the level of risk posed.

Automated triggers and alerts can mitigate the risk of the proceeds of crime being washed or spent in gaming machines. This provides the opportunity for staff to intervene.

[40] B2 gaming machines allow for a maximum stake of £100 and a maximum prize of £500.

[41] A new version of the licensing conditions and codes of practice (LCCP) comes into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

Additionally TITO has the potential to provide an audit trail for transactions particularly when used in conjunction with CCTV. Furthermore, some machines within the sector will reject dye stained notes, especially those heavily dyed, as well as fraudulent notes and coins.

The nature of the on-course environment mitigates much of the risk concerning cash transactions, for example, the risk appetite of many on-course operators limits the size of bets placed. Additionally, the transient nature of customers attending on-course events, and the limited number of on-course betting events taking place on any given day mitigates some of the risk.

Consequence
It is evident through casework and compliance activity that controls within the non-remote betting sector have not been robust enough to mitigate the risk of money laundering through the sector, albeit it is recognised that in the majority of cases this is through criminal spend.

Cash transactions by anonymous customers account for the vast majority of all non-remote transactions in the betting sector. It is the ability to remain anonymous, leaving no audit trail which reduces the risk to criminals who choose to launder or simply spend the proceeds of crime.

The Commission has identified cases where organised crime has sought to wash funds through this sector (including dyed notes, Scottish notes, and proceeds of crime in general), although in most cases the laundering was through criminal spend and not the 'washing' of dirty money.

The risk of the vulnerability being exploited received a rating of higher following the very high likelihood of occurrence and higher impact relative to other gambling sectors.