Regulatory settlement- Videoslots Limited

- Anti-money laundering – breaches of:
    - Licence condition 12.1.1.1 - Licensees must conduct an assessment of the risks of their business being used for money laundering and terrorist financing.
    - Licence condition 12.1.1.2 and 12.1.1.3 – Having regard to the risk assessment, licensees must have appropriate policies, procedures and controls to prevent money laundering and terrorist financing and such policies, procedures and controls are implemented effectively, kept under review and revised appropriately.
    - Licence condition 12.1.2 – Anti-money laundering measures for operators based in foreign jurisdictions requiring compliance with Money Laundering Regulations 2007 (superseded in 2017).
- Personal Management Offices – Breach of licence condition 1.2.1 requiring operators to ensure specified management offices are held by personal management licence (PML) holders.
- Key event notification - Breach of licence condition 15.2.1 relating to key event notifications in respect of reporting changes in the holders of management offices.
- Customer interaction – Failure to comply with code of practice - Social Responsibility Code 3.4.1. Compliance with a Social responsibility is a condition of the operating licence by virtue of section 82(1) of the Act.

Operators are expected to consider the issues here and review their own practices to identify and implement improvements in respect of the management of customers.

Executive summary

The Gambling Commission has completed an investigation which identified weaknesses in Videoslots Limited's (Videoslots) anti-money laundering and social responsibility controls.

The investigation followed a compliance assessment focussed on the measures that a remote gambling operator should have in place to address the prevention of money laundering and terrorist financing and compliance with related licence conditions. In carrying out the assessment, we also identified action that needed to be taken in respect of social responsibility (SR) code failures.

The identified failings raised significant concerns about the effectiveness of Videoslots' management and mitigation of risks to the licensing objectives in place at the time of the compliance assessment (September 2017). Videoslots had identified a number of issues and had started to implement improvements prior to the compliance assessment. Videoslots acknowledged its shortcomings at an early stage.

In line with our Statement of principles for licensing and regulation, Videoslots will pay a penalty package of £1,000,000 in lieu of a financial penalty. A breakdown of the regulatory settlement is set out below.

Findings

Breaches of licence condition 12.1.1.1 (Anti-money laundering) – Licensees must conduct an assessment of the risks of their business being used for money laundering and terrorist financing

Licence condition 12.1.1.1 came into effect from 31 October 2016 and requires an operator to assess the risks of their business being used for money laundering and terrorist financing. Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic, or any other material changes, and in any event reviewed at least annually. An appropriate risk assessment allows operators to identify risks relevant to their business, including the risks associated with the customers they transact with, and to conduct effective customer due diligence based on this assessment, among other things.

When we completed the assessment of 27 September 2017, we found that an appropriate risk assessment was not in place. Whilst it is accepted that Videoslots had carried out an assessment of risk in February 2017, it had not been formalised sufficiently to identify risk and mitigation to meet this requirement.

Breaches of licence condition 12.1.1.2 and 12.1.1.3 – Licensees must have appropriate policies, procedures and controls to prevent money laundering and terrorist financing and such policies, procedures and controls must be implemented effectively, kept under review and revised appropriately

Videoslots failed to establish and maintain appropriate risk-sensitive policies, procedures and controls relating to the management of its customers (including the monitoring and management of compliance with such policies and procedures) to prevent money laundering and terrorist financing, as required by licence conditions 12.1.1.2 and 12.1.1.3, and contrary to the requirements of regulation 19 of the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017 (the 2017 Regulations).

At the time of the assessment we found that Videoslots:

- conducted only basic checks on all customers, supported by a verification process once a deposit level of 2,000 Euros was reached in a 24-hour period. This approach to customer due diligence (CDD) is inadequate as it means that the same approach is adopted for all customers irrespective of the level of risk attributed to the customer.
- AML policies did not sufficiently define risk situations where enhanced customer due diligence and enhanced ongoing monitoring (EDD) would be required.
- the EDD process did not always include establishing the source of funds/source of wealth, as appropriate.

Videoslots did make some enquiries into the source of customer funds, such as requesting that customers verify the destination of withdrawals, generally by providing a copy of the relevant financial account documentation. Videoslots had taken steps to remedy the issue by inviting its customers to complete a declaration document outlining the source of funds, which it used as an indicator as to whether further enquiries were necessary, but further improvements were required.

Breaches of licence condition 12.1.2.1 – Anti-money laundering measures for operators based in foreign jurisdictions

Videoslots was required to put in place and implement the measures described in Parts 2 and 3 of the Money Laundering Regulations 2007 (superseded by the 2017 Regulations) insofar as they relate to casinos. We found that Videoslots had failed to sufficiently implement the measures as required.

The investigation highlighted that Videoslots failed to consistently apply EDD on a risk-sensitive basis, contrary to regulations 28 and 33 of the 2017 Regulations.

Regulation 28(11) of the 2017 Regulations required Videoslots to conduct ongoing monitoring of the business relationship, which includes scrutiny of the transactions undertaken by the customer throughout the course of the business relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the operator's knowledge of the customer and their risk profile. Regulation 33 of the 2017 Regulations includes the requirement to apply EDD, in addition to the measures required under regulation 28, in order to manage and mitigate the risks arising in situations where there is a high risk of money laundering or terrorist financing.

As examples:

- Customer A commenced gambling with Videoslots in November 2014. The customer subsequently deposited more than £211,000 and lost approximately £45,000 during game play. The initial checks carried out with the customer by Videoslots had revealed that the customer's bank account was overdrawn. As of November 2017, Videoslots' knowledge of the customer was reliant on identity documents and third-party assurances, where they should have undertaken enhanced customer due diligence measures (including establishing the source of the customer's funds).

- Customer B failed automated identity checks, resulting in the customer providing Videoslots with a fraudulent driving licence as evidence of their identity. In the initial stages this was not detected by Videoslots. The customer was then able to register multiple fraudulent bank cards, which was initially not detected. The bank cards were used to deposit and play large amounts of funds (for example £6,000 in one day in September 2017) without intervention by the operator. Videoslots' systems did, in due course, alert them to the activity, by which time the customer had made £17,405 in deposits, suspected to be the proceeds of crime.

In addition, at the time of the assessment, Videoslots did not sufficiently comply with the requirement to provide its relevant employees with training in how to recognise and deal with transactions, and other activities or situations which may relate to money laundering or terrorist financing (Regulation 24 of the 2017 Regulations). To comply with the 2017 Regulations, Videoslots should have provided relevant employees with regular training. For these purposes the Commission would include:

- the holders of all relevant personal management licences
- employees able to contribute to the identification and mitigation of the risk of money laundering or terrorist financing, such as those responsible for providing customer services and completing customer due diligence (CDD) measures.

Failure to comply Social Responsibility code 3.4.1 – Customer Interaction. Compliance with a Social responsibility code is a condition of the operating licence, by virtue of section 82(1) of the Act

Licensees must put into effect policies and procedures for customer interaction when they have concerns that a customer's behaviour may indicate problem gambling. SR code provision 3.4.1.1.e requires specific provision for making use of all relevant sources of information to ensure effective decision making, and to guide and deliver effective customer interaction, including in particular:

(i) provision to identify at risk customers who may not be displaying obvious signs of, or overt behaviour associated with, problem gambling; this should be by reference to indicators such as time or money spent.

(ii) specific provision in relation to customer designated by the Licensee as 'high value', 'VIP' or equivalent.

Commission officials found that at the time of the assessment (September 2017) Videoslots was in breach of 3.4.1.1.e. We noted that there were significant limitations in its ability to proactively identify and mitigate risk manifesting itself in terms of resource, systems, and controls.

As an example of our concerns, Customer C deposited £412,000 between 1 April 2016 and 31 January 2017, at which point the customer self-excluded. Videoslots' records did not show any evidence of customer interactions in respect of responsible gambling or indeed source of wealth. Videoslots is confident that its new policies and procedures would have addressed this issue.

Breach of Licence condition 1.2.1 – operating licence holders must ensure specified management offices must be held by personal management licence (PML) holders and Breach of licence condition 15.2.1 – Key event reporting

Licensees must ensure that individuals who occupy the management offices specified in respect of the licensed activities such as regulatory compliance hold a personal licence with the Commission authorising the performance of the functions of that office.

In addition, it is a requirement of licence condition 15.2.1.8.b to notify the Commission of the appointment of a person, or a person ceasing to occupy such, to a management position.

The Commission noted during its investigation that, for an 11-month period (2015/2016), an appropriate qualified individual occupying the regulatory compliance function did not hold a personal management licence and that the Commission had not always been notified of changes in individuals occupying management positions by way of key events.

Good practice

We consider that this case provides valuable learning for remote (online) and non-remote gambling operators. They should consider the following questions to address the issues identified in this case:

- Do you conduct appropriate assessments of the risks of money laundering and terrorist financing for your businesses, and implement policies, procedures and controls which manage the identified risks effectively?
- Do you have effective measures for customer due diligence, the ongoing monitoring of customers, and enhanced customer due diligence and enhanced ongoing monitoring which are sufficiently risk-focused, including the risk profiling of customers for these purposes?
- Are you ensuring that you can adequately evidence customer interactions?
- Do you have systems in place to ensure that your policies and procedures make specific provision for making use of all relevant sources of information where you have concerns that a customer's behaviour may indicate problem gambling? Are you putting into effect such policies and procedures?
- Are your customer interaction policies and procedures effective for your customers? Are you alert to the risk various customers bring?

- Are you providing your staff with appropriate training to ensure that they are aware of the law relating to money laundering and terrorist financing, and how to recognise and deal with transactions, activities or situations which may be related to money laundering or terrorist financing?
- Do you have sufficient resilience within your anti-money laundering and social responsibility functions with appropriately qualified individuals occupying specified management offices? Do those individuals hold personal management licences? Have you notified the Commission of any personnel changes in these specified management offices?

Useful guidance

How to comply with your anti-money laundering responsibilities

Social responsibility

Regulatory settlement

The regulatory settlement package consists of:

a) A payment in lieu of a financial penalty of £1,000,000 which will go to National Responsible Gambling Strategy project(s) to pay for research and treatment as determined appropriate to address the risk of harmful gambling. This payment includes a divestment in the sum of £310,478.08.

b) The voluntary placing of additional conditions on Videoslots' operating licence under section 117(1)(b) of the Act, requiring the licensee to:

- Maintain the appointment of an appropriately qualified Money Laundering Reporting Officer (MLRO) who holds a Personal Management Licence (PML), and, in appointing the MLRO, to ensure that the individual undertakes annual refresher training in AML and be able to evidence this to the Commission.
- Ensure that all PML holders, senior management and relevant employees undertake outsourced anti-money laundering training. All such staff must undertake outsourced refresher training annually thereafter.
- Continue to segregate funds as per licence condition 4.1 not lower than the level of 'medium' as defined by our guidance.
- Continue its review of the implementation and effectiveness of its AML and SR policies, procedures and controls, and, in addition, engage external auditors to sample the reviews that have been carried out so as to provide additional assurance in relation to the findings. The appointment and terms of reference of the external auditors must be agreed with the Commission.

c) Payment of £12,000 towards the Commission's investigative costs.

Conclusion

Our investigation found, and Videoslots accepts, that there were weaknesses in its systems relating to how it managed its customers for anti-money laundering and social responsibility purposes.

In determining the appropriate outcome, we took the following factors into account:

- Proactive and timely action taken by Videoslots to address all the issues identified

- Videoslots being open and transparent from the outset of the investigation and fully co-operative throughout
- A demonstrable insight into the seriousness of the failings.

Return to press release

Posted on 29 November 2018