

ISLE OF MAN
GAMBLING
SUPERVISION
COMMISSION



AML-CFT Guidance for
Software Suppliers 2020

V1.0 - 12/2020

Contents

Version Control	3
Abbreviations.....	4
About this document	5
About the GSC.....	6
Financial crime.....	6
Software supplier’s role in combatting crime.....	7
Risk Assessment	7
Reporting.....	8
Training	8
Nominated AML/CFT Officer.....	9
Summary	9
Resources	9

These notes are effective from December 2020

Version Control

Version	Date published	Comments
0.1	N/a	Draft circulated to AML Forum and terrestrial gambling operators for comment 25/11/2020.
1.0	Dec 2020	AML/CFT guidance published for OGRA software suppliers

Abbreviations

AML	Anti-money laundering
AML Forum	Regular forum hosted by the GSC for nominated officers and MLROs and AML/CFT Compliance Officers
CFT	Countering the financing of terrorism
FATF	The Financial Action Task Force
IOM FIU	Isle of Man Financial Intelligence Unit
FRSB	FATF Style Regional Body
GSC	The Gambling Supervision Commission which includes the Board of Commissioners and the Inspectorate
IOM	Isle of Man
MLRO	Money Laundering Reporting Officer
MONEYVAL	The Council of Europe's Committee of AML/CFT Experts, an FSRB
Nominated Officer	An employee nominated by a software supplier to be the point of contact for AML/CFT matters
OGRA	Online Gambling Regulation Act 2001
POCA	Proceeds of Crime Act 2008
Software Supplier	Any OGRA licence holder with the approved category L9a/L9b Software Supply and/or L9b Software Supply (Token-based)
The Code	The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism Code 2019
Tipping off	An offence committed by anyone within a regulated business of disclosing a suspicion of ML or TF to the suspect or a third party where that information is likely to prejudice an investigation

About this document

This document has been prepared by the Gambling Supervision Commission (GSC) and contains guidance for operators licensed under the Online Gambling Regulation Act 2001 (OGRA) approved for the supply of software only. Software suppliers are exempt from requirements set out under with the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019 (the Code)¹ in relation to anti-money laundering and countering the financing of terrorism (AML & CFT).

The guidance seeks to provide best practice for businesses that have no obligations under the Code but could still face the risk of liability for a substantive money laundering (ML) or terrorist financing (TF) offence.

In order to protect the reputation of the sector and facilitate good business practice, Software suppliers must comply with an additional licence condition outlined in Schedule 5 of their licence stating that the licensee shall disclose directly to the Isle of Man Financial Intelligence Unit (IOM FIU) –

- Any knowledge or suspicion of money laundering under the Proceeds of Crime Act 2008;
- Any knowledge or suspicion of terrorist financing under the Anti-Terrorism and Crime Act 2003;
- Information regarding unusual activity that may assist the IOM FIU in undertaking its functions under the Financial Intelligence Unit Act 2016.

AML/CFT guidance has been produced for OGRA licence holders who are obliged under the Code i.e. those that offer sports betting or casino products plus bookmakers and casinos. The full guidance is a bridge between the Code and the Financial Action Task Force (FATF) Recommendations. For further information on the FATF, and other external factors including MONEYVAL and the National Risk Assessment see the AML/CFT Guidance for Gambling Operators 2020.

The contents of this guidance should not be construed as legal advice.

¹ This includes a minor amendment to the AML/CFT Compliance Officer requirements via the AML/CFT (General and Gambling)(Amendment) Code 2019

About the GSC

The GSC is responsible for regulatory oversight of the gambling sector including operators' compliance with legislation such as the Gambling Acts and the Code. The GSC is an independent statutory board of Tynwald and comprises the Inspectorate and the board of the Commission.

The board of the Commission consists of several independent members drawn from various professions and backgrounds. The board of the Commission conduct monthly hearings into all matters that pertain to gambling in the Isle of Man and is supported by the Inspectorate.

The Inspectorate is managed by the Chief Executive of the GSC.

The GSC is available 9:00am to 5:00pm Monday to Friday and can be contacted via phone on +44 (0)1624 694331, via e-mail on gaming@gov.im or at the postal address below—

Ground Floor,
St. George's Court,
Myrtle Street,
Douglas
IM1 1ED

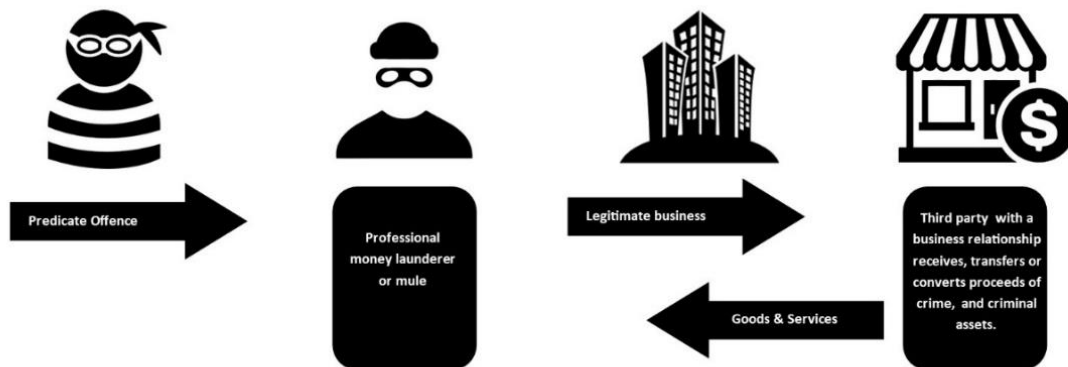
Financial crime

Criminals, including terrorists, attempt to use the world's financial systems in order to benefit from crime or fund projects designed to further their causes, sometimes resulting in further criminality or acts of terror. Some terrorist organisations have an interest in obtaining weapons of mass destruction (so called chemical, radiological, biological and nuclear devices) for the purposes of terrorism and so the failure to prevent terrorist financing can have particularly serious consequences for society as a whole.

To combat this activity, an alliance of the world's governments cooperates on initiatives to counter money laundering and the financing of terrorism. The compliance of each nation is monitored and those that fail to cooperate may be subject to international sanction.

The interception of money laundering is referred to in this document as AML (anti money laundering). The interception of terrorist financing and the prevention of the proliferation of weapons of mass destruction is referred to as CFT (combating the financing of terrorism).

Software supplier's role in combatting crime



Schedule 4 of the Proceeds of Crime Act 2008 (POCA) outlines that the Code applies to businesses conducting online gambling within the definition of OGRA, ensuring that businesses have controls in place to identify ML and TF risks and deal with them accordingly. However, Schedule 4 does not apply where business is being carried out by a software supplier.

Any business could have liability where they have failed to report any suspicions or knowledge of an offence and as a licence holder, the GSC would expect any business to maintain the reputation of the sector and the island and comply fully with all licence conditions. In order to do so the GSC recommend that take the following steps to facilitate the identification and reporting of suspicious behaviour.

The graphic above shows an example of how proceeds of crime could be laundered through legitimate businesses that have little or no AML/CFT controls, or that have been set up to facilitate ML or TF, and how those proceeds of crime could be passed on to a business partner.

Example - a drug distribution ring needs to conceal payments and uses a professional money launderer who has set up an online gambling business to make payments look like legitimate income. The business to create further legitimacy collaborates with a software provider, utilising their platform on a revenue share system to enable genuine play and conceal proceeds of crime. Unknowingly the software provider facilitates the movement of proceeds of crime through its third party business arrangement.

The use of legitimate business for money laundering may have red flag indicators, such as large regular deposits and losses outside of normal patterns that could be identified through product monitoring by third parties. Other red flags may be that the business is situated within a jurisdiction with known poor AML/CFT controls, that the business structure is overly complicated or involves nominee shareholders or that the business is unwilling to provide due diligence.

Risk Assessment

It is important to understand the risks within a business in order to put in policies and procedures to mitigate risk and establish appropriate internal controls. It is recommended that software supply licence holders carry out an AML/CFT Risk Assessment of their own business that could take into consideration the following—

- The vulnerabilities of products, goods or services to ML/TF abuse;
- The jurisdictional risks when forming third party relationships;
- The level of due diligence that should be undertaken when forming contractual relationships;
- What further checks should be carried out on third parties where potential risk has been identified, such as adverse media, sanctions checks etc;
- Assessment of technological developments for vulnerability to ML and TF use.

Reporting

Under Section 141 of POCA any person commits an offence by acquiring criminal property, using criminal property or having possession of criminal property. It is also an offence under section 139 of POCA to conceal, disguise, convert, transfer or remove criminal property.

This means that if a software supplier were to accept payment from a company where they suspect criminality then they themselves would be committing a money laundering offence.

It should be noted that money laundering is not only confined to transactions involving money but can also include any benefit of crime including assets. Businesses would have a defence against any liability where knowledge or suspicion of a crime had been reported appropriately and consent obtained for any transaction to continue.

Software supply licence holders have an obligation outlined in Schedule 5 (6) of licence conditions to disclose any knowledge or suspicion of ML or TF and any information regarding unusual activity to the IOM FIU.

For more information on reporting, see Part 5 of AML/CFT Guidance for Gambling Operators 2020.

Training

All staff within a business can report suspicions or knowledge and it is essential that staff understand what ML or TF could look like, how to report and who to report to within a business.

All businesses should put in place procedures to ensure that the subject of any report or suspicion is not alerted to the suspicion (this is known as tipping off). Although software suppliers may not be held liable under POCA for a tipping off offence due to their status, they could still be held accountable for prejudicing an investigation if tipping off were to occur.



Nominated AML/CFT Officer

Software supplier licence holders are required through Schedule 5(6) of licence conditions to nominate an individual to be the focal point for any ML or TF concerns, fulfil any reporting requirements, consider staff training and undertake risk assessments. It is important that the nominated officer meets the following requirements—

- Competent – has knowledge and understanding, ideally with experience of AML/CFT and reporting
- Sufficiently resourced and supported – can implement appropriate internal control mechanisms and has sufficient oversight and time to carry out any duties
- Seniority or sufficient access – the nominated officer must be able to make and implement recommendations in line with the business' risk assessment.

Summary

This guidance is for software supply licence holders who have no other category on their licence. Where other categories are held on an OGRA licence alongside software supply the AML/CFT Guidance for Gambling Operators 2020 should be referred to for a full overview of requirements.

Software supply licence holders exempted from the requirements of the Code are still required to report any knowledge or suspicions of ML or TF to the IOM FIU through Schedule 5(6) of their licence conditions or any information of unusual activity that may assist the FIU in undertaking its functions under the Financial Intelligence Unit Act 2016.

Through licence conditions, software supply licence holders are required to have a nominated officer to act as a focal point for reporting and monitoring. A nominated officer should be sufficiently senior, adequately resourced and have some experience and/or understanding of AML/CFT matters.

By applying good practice in relation to ML and TF risks businesses can—

- Decrease the regulatory burden by ensuring compliance and avoiding enhanced supervision and remediation;
- Increase the positive reputation of the sector which in turn will grow business opportunities;
- Meet social responsibility goals by contributing to the safety of the community;
- Support global initiatives to reduce crime and terror;
- Safeguard the business and employees against risk and employees and criminal; liability.

Resources

The GSC produce full guidance on our website for all licence holders and hold regular AML forums for nominated officers and MLROs to attend. Below is a list of hyperlinks to other useful resources.

- [FATF website](#)
- [Moneyval](#)
- [Mutual Evaluation Report Isle of Man 2016](#)
- [Isle of Man National Risk Assessment 2020](#)

- [AML/CFT Online Guidance 2015](#)
- [Isle of Man Financial Crime Strategy 2017-2020](#)
- [AML/CFT Guidance for Virtual Currencies](#)
- [AML/CFT Supplementary Guidance 2018](#)