GAMBLING COMMISSION

Anti-money laundering: Suspicious activity reporting requirements for remote operators

Advice note, September 2014

1 Introduction

1.1 This advice note provides information on suspicious activity reporting requirements, particularly where the licensed operator is based in a foreign jurisdiction, following the implementation of the Gambling (Licensing and Advertising) Act 2014.

1.2 It is intended to assist remote operators in determining to which body or Financial Intelligence Unit (FIU) known or suspected money laundering activity should be reported, and the circumstances in which appropriate consent should be sought.

2 Summary

2.1 The note explains what remote operators licensed by the Gambling Commission (the Commission) are required to do in relation to reporting suspicious activity, and in relation to obtaining consent to proceed with customer transactions which may result in money laundering offences.

2.2 In summary, remote operators licensed by the Commission are required to:

- report suspicious activity to the FIU in the country in which the remote gambling equipment is located, if that FIU is a member of the Egmont group and the country has not excluded or prohibited remote gambling
- in all other cases, report suspicious activity to the National Crime Agency (NCA)
- provide the Commission with the NCA or, where available, the relevant FIU unique reference number of the suspicious activity report (SAR) within five days
- seek consent to proceed with a 'prohibited act' from the NCA for transactions involving British customers.

2.3 The following paragraphs explain the detail and reasoning behind these propositions.

3 Legal provisions

The Proceeds of Crime Act 2002

3.1 The Proceeds of Crime Act 2002 (POCA)[1] imposes duties on all gambling operators in the United Kingdom (UK)[2] to:

- make disclosures in the prescribed form and manner
- obtain appropriate consent to do a prohibited act (as defined below), where appropriate.

[1] As amended: see in particular the Serious and Organised Crime and Police Act 2005 ('SOCPA'), ss.102(1) and (5), 104(1) to (3), 105(1) and (2), 106(1) and (2) and 174(2), and Sched. 17, Pt 2; the Proceeds of Crime Act 2002 and Money Laundering Regulations 2003 (Amendment) Order 2006 (S.I. 2006 No. 308), art. 2; the Serious Crime Act 2007 ('SCA'), s.74(2), and Sched. 8, paras 121 and 126; and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (S.I. 2007 No. 3398); and the Crime and Courts Act 2013, s.15(3), and Sched. 8, paras 108 and 129; Proceeds of Crime Act 2002 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 (S.I. 2007 No. 3287).

[2] United Kingdom of Great Britain and Northern Ireland.

Victoria Square House
Victoria Square
Birmingham B2 4BP

T 0121 230 6666
F 0121 230 6720
www.gamblingcommission.gov.uk

3.2 POCA also defines various money laundering offences: concealing, disguising, converting, transferring criminal property, or removing criminal property from the United Kingdom[3]; entering into an arrangement which is known or suspected to facilitate the acquisition, retention, use or control of criminal property by or on behalf of another person[4]; and the acquisition, use or possession of criminal property[5]. These are referred to collectively in the legislation as 'prohibited acts'.

3.3 It is a defence to a money laundering offence under POCA to make an 'authorised disclosure' and (if the disclosure is made before any act described in the preceding paragraph is carried out) to obtain the 'appropriate consent' before dealing with the criminal property[6].

3.4 The offences of money laundering and the duty to report under POCA apply in relation to the proceeds of any criminal activity, wherever conducted, including abroad, that would constitute an offence if it took place in the UK[7]. However, a person does not commit an offence where it is known or believed, on reasonable grounds, that the relevant criminal conduct occurred outside the UK and the relevant conduct was not criminal in the country where it took place and is not of a description prescribed by an order made by the Secretary of State[8].

3.5 Currently, offences committed overseas which the Secretary of State has prescribed by order described in the preceding paragraph as remaining within the scope of the duty to report under POCA, are those which are punishable by imprisonment for a maximum term in excess of 12 months in any part of the UK if they occurred there, other than overseas conduct that would constitute an offence under the Gaming Act 1968; an offence under the Lotteries and Amusements Act 1976; or an offence under sections 23 or 25 of Financial Services and Markets Act 2000[9].

Suspicious activity reports

3.6 POCA requires the disclosure of information to the NCA by an operator either directly by its employees or through the operators 'nominated officer'.

3.7 The requirement to disclose arises in a number of situations, the first two of which discussed below apply to gambling operators in the 'regulated sector' (which in the context of this advice note means a remote or land-based casino[10]).

3.8 A person employed by an operator conducting business in the regulated sector is required to make a disclosure to the operator's nominated officer[11] or to the NCA if he or she knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering. Failure to make such a disclosure may be a criminal offence, which may be committed negligently.[12]

3.9 The nominated officer referred to in the preceding paragraph and working in the regulated sector is also required to make a disclosure to the NCA of the information provided to him or her in that regard if it causes knowledge or suspicion that another person is engaged in money laundering. Again, failure to make such a disclosure may amount to a criminal offence, which may be committed negligently.[13]

3.10 The following requirements apply to all gambling operators and their employees, whether or not they are working in the regulated sector.

---

[3] Section 327 of POCA.
[4] Section 328 of POCA.
[5] Section 329 of POCA.
[6] Sections 327, 328 and 329 of POCA.
[7] Section 340 of POCA.
[8] Sections 327, 328 and 329 of POCA.
[9] The Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006.
[10] See Schedule 9 of POCA, as amended by Proceeds of Crime Act 2002 (Business in the Regulated Sector and Supervisory Authorities) Order 2007 (S.I. 2007 No. 3287).
[11] See section 330(9) and 340(11) of POCA.
[12] See section 330 of POCA.
[13] See section 331 of POCA

3.11 If a person knows or suspects that he or she is about to deal with criminal property (in other words if that person believes that he or she is about to commit one of the principal money laundering offences under sections 327, 328 or 329 of POCA) then it may be a defence to such an offence if that person makes an 'authorised disclosure' and, if the authorised disclosure is made before the transaction takes place, that he or she has the 'appropriate consent' to conduct it.

3.12 An authorised disclosure is one made by the operator's employee to the NCA, or to the operator's nominated officer that the property in question is criminal property.[14] The nominated officer who receives an authorised disclosure is required to make a disclosure to the NCA of the information provided to him in that regard if it causes knowledge or suspicion that another person is engaged in money laundering. Failure to do so may amount to a criminal offence.[15]

3.13 A disclosure to the NCA in all cases is commonly known as a 'suspicious activity report' (or SAR) and should be made in the prescribed form.[16]

3.14 Further information regarding the suspicious activity reporting requirements under POCA can be found in the Commission's guidance *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*, and in *Duties and responsibilities under the Proceeds of Crime Act 2002 - Advice for operators (excluding casino operators).*[17]

Appropriate consent

3.15 The statutory mechanism under POCA, which allows the NCA to grant permission for a 'prohibited act' by an operator to go ahead where the operator deals with criminal property, is known as 'appropriate consent'[18] and may provide the operator with a defence against prosecution for committing a prohibited act. As noted above, where an operator fails to obtain appropriate consent from the NCA, the operator or its employees may be committing a money laundering offence. In order to obtain the appropriate consent, the operator must make an authorised disclosure to the NCA.

3.16 The decision by an operator whether to obtain appropriate consent will arise where the operator believes that, by proceeding with a customer transaction, they will be concealing, disguising, converting, transferring or removing criminal property; facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person; or acquiring, using or possessing criminal property.

3.17 Further information regarding appropriate consent under POCA can be found in the Commission's guidance *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*, and in *Duties and responsibilities under the Proceeds of Crime Act 2002 - Advice for operators (excluding casino operators).*[19]

Tipping off and prejudicing an investigation

3.18 It is an offence to disclose to any person that a report has been made to the NCA, or that an investigation is taking place into allegations of money laundering, if such disclosure is (as a matter of fact) likely to prejudice an investigation which is being or might be conducted (i.e. whether or not it is known or suspected that the disclosure is likely to cause such prejudice)[20]. It is also an offence to falsify, conceal, destroy or otherwise dispose of documents relevant to such an investigation.[21]

---

[14] See section 338 of POCA
[15] See section332 of POCA.
[16] See section 339 of POCA. See also http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/specialist-capabilities/ukfiu/seeking-consent-for-financial-transactions
[17] Available from www.gamblingcommission.gov.uk
[18] Section 335 of POCA.
[19] Available from www.gamblingcommission.gov.uk
[20] Section 333A of POCA
[21] Section 342 of POCA

Application of the Gambling Act

3.19 Section 36 of the Gambling Act 2005 (the Act), as amended by the Gambling (Licensing and Advertising) Act 2014, applies the requirement to obtain an operating licence to the provision of remote gambling facilities where:

- at least one piece of remote gambling equipment used in the provision of the facilities is situated in Great Britain (Britain)[22], or
- no remote gambling equipment is situated in Britain, but the facilities are used there (where the person providing the facilities knows or should know that the facilities are being used, or are likely to be used, in Britain).

3.20 The determining factors for licensing purposes are therefore the location of the remote gambling equipment and the location of the customer using the remote gambling facilities. If either of these locations is Britain, then a licence issued by the Commission is required to provide remote gambling facilities.

3.21 'Remote gambling equipment' is defined as electronic or other equipment used by or on behalf of a person providing facilities for remote gambling to:

- store information relating to a person's participation in remote gambling
- present, to persons who are participating or may participate in the gambling, a virtual event or process by reference to which the gambling is conducted
- determine all or part of a result or of the effect of a result
- to store information relating to a result.[23]

3.22 For the purposes of this advice note, 'British customer' is inferred to mean a customer who is physically located in Britain when they use gambling facilities provided in reliance on a licence issued by the Commission, regardless of their usual residential address.

3.23 'Non-British customer' on the other hand means a customer who is *not* physically located in Britain when they use gambling facilities provided in reliance on a licence issued by the Commission, regardless of their usual residential address.

Applicability of POCA

3.24 The Commission considers that the anti-money laundering provisions in Part 7 of POCA[24] apply to all remote operators where, in each case, they either have:

- British customers, or
- remote gambling equipment located in Britain.

3.25 The Commission thus expects such operators to comply with the anti-money laundering provisions of that legislation.

3.26 A key requirement of the legislation is for all remote operators to report known or suspected money laundering activity.

4 The FATF Recommendations and the EU Directive

4.1 The Financial Action Task Force (FATF), which is the organisation which sets global standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system, recommend that suspicious activity should be reported promptly 'to the financial intelligence unit (FIU)'[25].

4.2 The EU Directive[26] sets out a framework which is designed to protect the European financial system against the risks of money laundering and terrorist financing and is, to a large extent, based on the international standards adopted by FATF. It requires EU

[22] England, Scotland and Wales.
[23] Section 36(4) and (5) of the Act.
[24] i.e. sections 327 to 340 of POCA.
[25] Recommendation 20 of the FATF Recommendations: International standards on combating money laundering and the financing of terrorism & proliferation.
[26] Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

member states to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions (including remote and land-based casinos), to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities. The UK legislation referred to above implements those requirements.

4.3 The EU Directive requires that SARs are submitted to 'the FIU of the member state in whose territory the institution or person forwarding the information is situated'[27].

5 Egmont Group of Financial Intelligence Units

5.1 The Egmont Group of Financial Intelligence Units (the Egmont Group) was established as an informal network of FIUs for the stimulation of international co-operation. The Egmont Group FIUs meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the areas of information exchange (including SARs), training and the sharing of expertise.

5.2 The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to support the implementation of domestic programs in this field.

5.3 The Egmont Group has created a secure encrypted capability to share information over the Internet. The Secure Web system (the ESW) permits members of the Group to communicate with one another via secure email. Egmont Group members are able to exchange operational information in a secure way, which can be acted upon appropriately and timeously.

Egmont Group membership

5.4 The following FIUs are currently members of the Egmont Group:

Afghanistan (FinTRACA)	Albania (GDPML)	Algeria (CTRF)
Andorra (UPB)	Anguilla (MLRA)	Antigua and Barbuda (ONDCP/FIU)
Argentina (UIF)	Armenia (FMC)	Aruba (MOT)
Australia (AUSTRAC)	Austria (A-FIU)	Azerbaijan (FMS)
Bahamas (FIU-Bahamas)	Bahrain (FID)	Bangladesh (BFIU)
Barbados (FIU-Barbados)	Belarus (DFM)	Belgium (CTIF-CFI)
Belize (FIU-Belize)	Bermuda (FIA)	Bolivia (UIF)
Bosnia & Herzegovina (FID)	Brazil (COAF)	British Virgin Islands (FIA)
Bulgaria (FID-SANS)	Burkina Faso (CENTIF-BF)	Cameroon (NAFI)
Canada (FINTRAC-CANAFE)	Cayman Islands (CAYFIN)	Chile (UAF)
Colombia (UIAF)	Cook Islands (CIFIU)	Costa Rica (UIF)
Croatia (AMLO)	Curaçao (FIU-Curaçao)	Cyprus (MOKAS)
Czech Republic (FAU-CR)	Denmark (FIU Denmark)	Dominica (FIU-Dominica)
Egypt (EMLCU)	El Salvador (UIF-El Salvador)	Estonia (MLIB)
Fiji (Fiji-FIU)	Finland (RAP)	France (TRACFIN)
Gabon (ANIF)	Georgia (FMS-Georgia)	Germany (FIU)
Gibraltar (GCID GFIU)	Greece (HELLENIC FIU)	Grenada (FIU-Grenada)
Guatemala (IVE)	Guernsey (FIS)	Holy See (VCS) (AIF)
Honduras (UIF-Honduras)	Hong Kong (JFIU)	Hungary (HFIU)
Iceland (RLS)	India (FIU-IND)	Indonesia (PPATK)
Ireland (MLIU)	Isle of Man (FCU-IOM)	Israel (IMPA)
Italy (UIF)	Ivory Coast (CENTIF-CI)	Japan (JAFIC)
Jersey (FCU-Jersey)	Jordan (AMLU)	Kazakhstan (Finmonitoring)
Korea, Republic of (KoFIU)	Kyrgyz, Republic (FIS)	Latvia (KD)
Lebanon (SIC)	Liechtenstein (EFFI)	Lithuania (FCIS)
Luxembourg (FIU-LUX)	Macao (GIF)	Macedonia (MLPD)
Malawi (FIU-Malawi)	Malaysia (UPWBNM)	Mali (CENTIF-Mali)
Malta (FIAU)	Marshall Islands (DFIU)	Mauritius (FIU-Mauritius)
Mexico (FIU-Mexico)	Moldova (SPCSB)	Monaco (SICCFIN)
Mongolia (FIU-Mongolia)	Montenegro (APMLTF)	Morocco (UTRF)
Netherlands (FIU-NL)	New Zealand (NZ-Police FIU)	Nigeria (NFIU)
Niue (Niue FIU)	Norway (EFE)	Panama (UAF-Panama)
Paraguay (UAF-SEPRELAD)	Peru (UIF-Peru)	Philippines (AMLC)
Poland (GIFI)	Portugal (UIF-Portugal)	Qatar (QFIU)
Romania (ONPCSB)	Russia (Rosfinmonitoring)	Samoa (SFIU)

[27] Article 22(2).

San Marino (FIA San Marino)	Saudi Arabia (SAFIU)	Senegal (CENTIF)
Serbia (APML)	Seychelles (Seychelles FIU)	Singapore (STRO)
Slovakia (FSJ)	Slovenia (OMLP)	Solomon Islands (SIFIU)
South Africa (FIC)	Spain (SEPBLAC)	Sri Lanka (Sri Lanka FIU)
St. Kitts & Nevis (FIU-SKN)	St. Lucia (FIA-St. Lucia)	St. Vincent & Grenadines (FIU-SVG)
Sweden (NFIS)	Switzerland (MROS)	Syria (CMLC)
Taiwan (AMLD)	Tajikistan (FMD)	Thailand (AMLO)
Togo (CENTIF-Togo)	Trinidad and Tobago (FIUTT)	Tunisia (CTAF)
Turkey (MASAK)	Turks & Caicos (FCU)	Ukraine (SFMS)
United Arab Emirates (AMLSCU)	United Kingdom (NCA)	United States (FinCEN)
Uruguay (UIAF)	Uzbekistan (FIU-Uzbekistan)	Vanuatu (FIU-Vanuatu)
Venezuela (UNIF)		

5.5 While this list of member FIUs is extensive, some jurisdictions do not include gambling businesses under their anti-money laundering or counter terrorist financing legislation, or they may prohibit online gambling altogether.

6 Ordinary code provisions

6.1 Two ordinary code provisions in the *Licence conditions and codes of practice* state that operators should have regard for the Commission's guidance or advice on anti-money laundering. The provisions are different for remote casino operators and other remote gambling operators, as explained below.

Remote casino operators

6.2 Ordinary code provision 2.1.1 states that remote casino operators should act in accordance with the Commission's guidance on anti-money laundering, *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*, in order to help prevent activities related to money laundering and terrorist financing.

Other remote operators

6.3 Ordinary code provision 2.1.2 states that all remote operators, other than remote casino operators, should take into account the Commission's advice on the Proceeds of Crime Act 2002, *Duties and responsibilities under the Proceeds of Crime Act 2002 - Advice for operators (excluding casino operators)*, as part of their procedures for compliance with the requirements in respect of the prevention and detection of money laundering in POCA.

6.4 Both documents referred to in the preceding paragraphs explain the requirement for operators to report known or suspected money laundering activity to the NCA.

7 New licence requirement

7.1 Amended licence condition 15.2.1, which came into force (as amended) on 4 August 2014, requires all gambling operators to inform the Commission of the unique reference number issued by the UKFIU[28] of the NCA in respect of each SAR submitted by the operator within five working days of receipt of the unique reference number.

8 Reporting requirements for remote operators

8.1 The Commission is mindful that some remote operators not physically located in Britain may be required by local law to report instances of known or suspected money laundering activity by British customers to the FIU of the jurisdiction in which the operator is situated, rather than the NCA.

8.2 Commission is thus of the view that remote operators should report suspicious activity to the authorities in the area where the remote gambling equipment used in the specific suspicious transaction is located. However, in relation to transactions concerning British

[28] The UK Financial Intelligence Unit, which is the unit within the NCA that operates the disclosure and consent regime for money laundering in the UK.

customers it is also of the view that such reports should also be received by the authorities in this jurisdiction.

8.3 Having regard to the matters discussed above, the Commission therefore explains as follows in respect of the reporting by remote operators of known or suspected money laundering activity, and requests for appropriate consent.

Suspicious activity reporting

8.4 Where any of the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located in Britain (as well as equipment located in Northern Ireland), the known or suspected money laundering activity must be reported to the NCA. Operators must provide the Commission with the unique reference numbers allocated by the UKFIU of the NCA, for reports submitted by them, within five days of receipt thereof, in accordance with licence condition 15.2.1.

8.5 Where the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located outside Britain, but involves a British customer, and the jurisdiction in which the equipment is located is not a member of the Egmont Group (or the jurisdiction does not include gambling businesses under its anti-money laundering or counter terrorist financing legislation, or prohibits online gambling), the known or suspected money laundering activity must be reported to the NCA. Operators must provide the Commission with the unique reference numbers allocated by the UKFIU of the NCA, for reports submitted by them, within five days of receipt thereof, in accordance with licence condition 15.2.1.

8.6 In all other cases, the known or suspected money laundering activity must be reported to the FIU of the jurisdiction in which the remote gambling equipment used in a transaction, which is known or suspected to involve money laundering, is located. The relevant report will then be shared with the NCA through the Egmont Group, where appropriate. Where circumstances permit, operators should provide the Commission with the unique reference numbers allocated by the applicable FIU, for reports concerning British customers, within five days of receipt thereof.

8.7 These reporting requirements are summarised in the table below:

Customer	Location of remote gambling equipment	Member of Egmont Group?	Report suspicious activity to	Unique reference numbers (URNs)
British or Non-British customer*	Britain** or Northern Ireland	Yes	NCA	Operators should provide the Commission with the URNs allocated by the NCA within five working days
British customer*	Outside Britain**	No	NCA	Operators should provide the Commission with the URNs allocated by the NCA within five working days
		Yes, but domestic FIU does not receive gambling SARs		
		Country prohibits online gambling		
British or Non-British customer*	Outside Britain**	Yes	Domestic FIU	Where circumstances permit, operators should provide the Commission with the URNs allocated by the FIU, for reports concerning British customers, within five working days

* see paragraphs 3.22 and 3.23

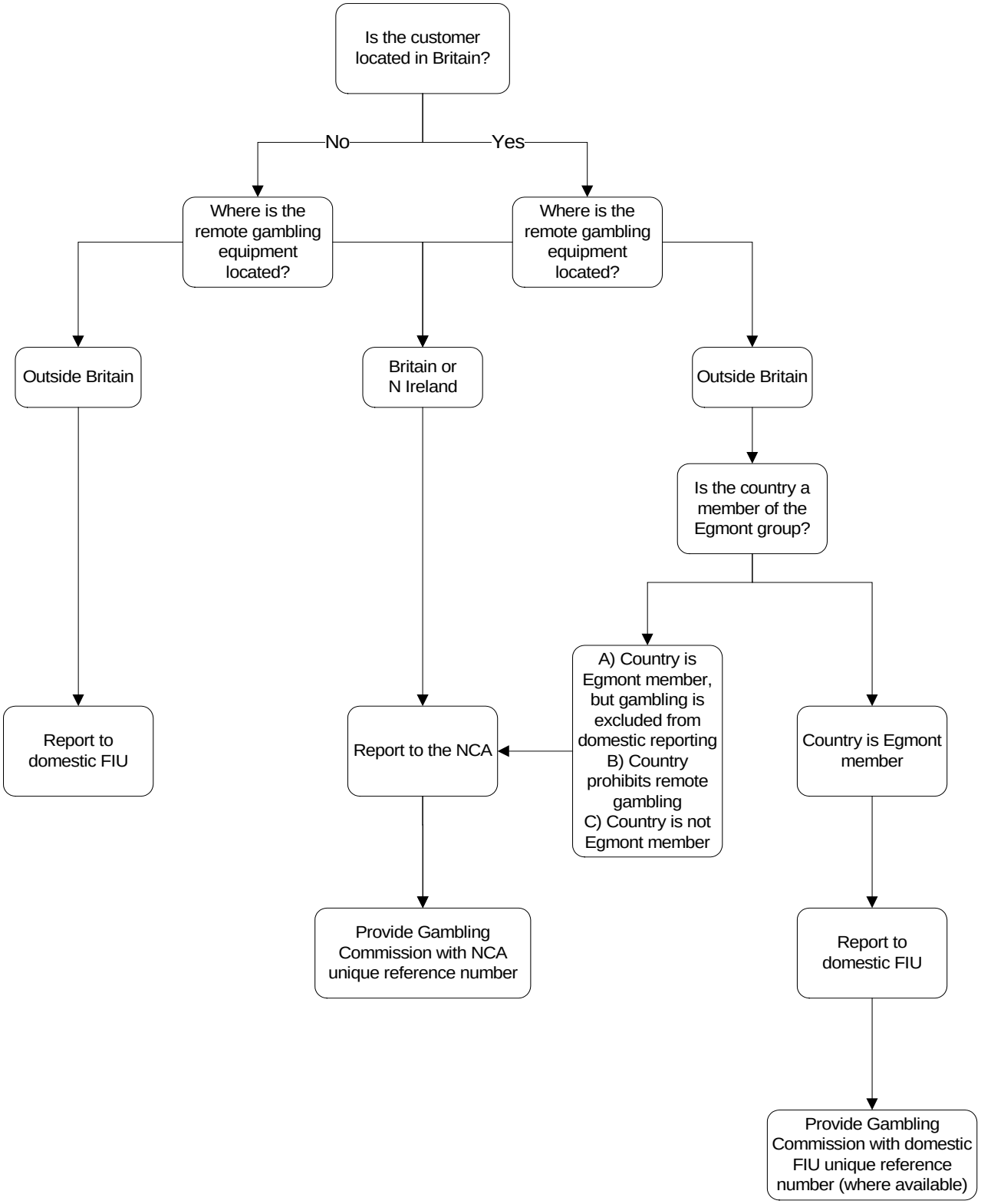
** Britain means England, Scotland and Wales

Appropriate consent

8.8 Where remote operators wish to make use of the defences provided by sections 327(2)(a), 328(2)(a) and 329(2)(a) of POCA where they believe that, by proceeding with a transaction with a British customer, they will be committing a prohibited act[29], they should seek appropriate consent, in accordance with section 335 of POCA, from the NCA.

[29] See paragraphs 3.15 and 3.16.

Annex – Flowchart of suspicious activity reporting



Gambling Commission September 2014

Keeping gambling fair and safe for all

Gambling Commission
Victoria Square House, Victoria Square
Birmingham B2 4BP

T 0121 230 6666 **F** 0121 230 6720 **E** info@gamblingcommission.gov.uk **ADV 14/08**