



ANTI-MONEY LAUNDERING POLICY

1.0 INTRODUCTION

1.1 InterGlobal is a UK registered specialist insurance company that provides international private medical insurance for expatriates, frequent travellers and students worldwide. Its head office is in the UK and it has representative offices and associated companies in various locations worldwide. It conducts insurance business both direct with policyholders and through intermediaries. Its products are offered to clients through a variety of media including on-line sales. InterGlobal holds licences in some overseas countries and provides policies direct to clients in these jurisdictions, either direct or through representative and subsidiary offices in the regions. In other jurisdictions, its products are offered through locally licensed insurers.

Private Medical Insurance is a low risk product due to the nature of the policy. It does not have an investment element, has no cash in value and is usually taken out by individuals for themselves and their families or by employers for their staff members. However, some of the jurisdictions in which InterGlobal's products are sold may present a risk element for various reasons.

Non-investment general insurance business is not currently covered under the FSA's Money Laundering rules. However, InterGlobal is subject to the FSA's SYSC Rules requiring businesses to have adequate systems and controls in place to manage risks and their business affairs, and as a UK business, it is subject to the Proceeds of Crime Act 2002 (POCA), the Terrorism Act 2000 and other legislation. InterGlobal also follows guidance provided by the Financial Action Task Force (FATF) on Money Laundering and other industry guidance.

2.0 SCOPE OF THE POLICY

2.1 This Policy applies to all employees of InterGlobal including temporary staff and contractors working for the company worldwide. The Policy sets out the procedures which must be followed to enable InterGlobal comply with relevant legislation and its other obligations.

2.2 Failure to comply with this Policy and the Company's Anti-Money Laundering procedures may lead to disciplinary action being taken against employees.

3.0 PURPOSE

3.1 This Policy is intended to enable InterGlobal to meet its compliance requirements in a way which is proportionate to the low risk nature of the business type and the higher risk level of the types of jurisdictions that it operates in.

- 3.2 To set out the Company's policy and make all employees aware of the legislative changes that have been made, their responsibilities regarding these changes, and the consequences of non compliance with this policy.
- 3.3 Potentially any employee could be caught by the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. Internal guidance notes and training material give practical examples of how money laundering could occur within the business.
- 3.4 Whilst the risk of InterGlobal contravening the legislation is low, it is extremely important that all employees are familiar with their legal responsibilities and how it Money laundering could impact upon the business.

4.0 MANAGEMENT RESPONSIBILITIES : THE MONEY LAUNDERING REPORTING OFFICER

- 4.1 The officer nominated to receive disclosures about money laundering activity within InterGlobal is the Group Legal and Compliance Director who is also the Company's Money Laundering Reporting Officer (MLRO).
- 4.2 Anti-Money Laundering is incorporated into the systems and processes of the firm at Account Opening, Client Services and after-sales during the claims and refund process.
- 4.3 Training and awareness programmes are provided for new and existing temporary and permanent staff and processes are constantly reviewed by the Legal and Compliance function who are also available to give advice as required.
- 4.4 The Finance, Operations, Client Services and Credit Control business heads are the Departmental contacts authorised by the MLRO to facilitate relevant procedures and act on behalf of the MLRO when considering whether a disclosure needs to be made and how to embed the procedures within the business.
- 4.5 Overall responsibility for Money Laundering sits with the board and any issues and risks are reported via the regular Board meetings and related Executive Committees.

5.0 SUSPICIOUS ACTIVITY REPORTING

Reporting to the Money Laundering Reporting Officer

- 5.1 InterGlobal's procedures require employees to report any suspicions through previously advised channels to the Money Laundering Reporting Officer.
- 5.2 Employees are made aware through training and awareness programmes and existing procedures about the offences of 'tipping off' and other offences related to this.
- 5.3 Staff are mandated to report suspicions as soon as practicable where they know or suspect that money laundering activity is taking or has taken place, or if they become concerned that their involvement in a transaction brought by a client may amount to a prohibited act under the legislation. Disclosure is made using existing forms and employees are required to give as much information as possible within the forms. Details will include full name, address, date of birth, whether an offence is suspected and details of the transaction. Where employees are concerned that their involvement in a transaction could amount to a prohibited act under sections 327 – 329 of the POCA 2002, then their report must include all relevant details as consent may be required from the Serious Organised Crime Agency (SOCA), via the MLRO, for the transaction to continue.

5.4 Once the matter has been reported to the MLRO, employees are required to take further directions from the MLRO and are required to undertake no further investigations into the matter. The MLRO will decide whether a disclosure to the authorities is required and in turn refer the matter to the SOCA, if appropriate.

5.5 Employees must not voice suspicions to the person (s) to whom they suspect of money laundering, even if they have received confirmation from the MLRO that the SOCA has given consent to a particular transaction proceeding, as this may result in the commission of the offence of 'tipping off'.

6.0 MONEY LAUNDERING REPORTING OFFICER: ACTIONS UPON RECEIPT OF A DISCLOSURE

6.1 Upon receipt of a disclosure report, the MLRO will note the date of receipt, acknowledge receipt and advise the relevant employee of the timescale within which a response will be given.

6.2 The MLRO will consider the report and any other available relevant internal information such as:

- transaction patterns and volumes;
- the length of relevant business relationships;
- the number of one-off transactions and linked one-off transactions;
- any identification evidence held;

and undertake such other reasonable inquiries as may be appropriate in order to ensure that all available information is taken into account in deciding whether to lodge a Suspicious Activity Report (SAR) with the Serious Organised Crime Agency (SOCA). Such enquiries must be made in such a way as to avoid any appearance of 'tipping off' those involved. The MLRO may also need to discuss the report with the employee.

6.3 Upon completion of the evaluation, a determination will be made as to whether:

- there is actual or suspected money laundering taking place; or
- there are reasonable grounds to know or suspect that is the case; and
- whether consent is required from the SOCA for a particular transaction to proceed.

6.4 If a conclusion is reached to report, then it will be made as soon as practicable to the SOCA in the prescribed form, unless exemptions to disclosure apply (e.g. legal professional privilege) in which case the report will be noted accordingly and appropriate action taken.

6.5 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then consent will be given for any ongoing or imminent transaction(s) to proceed.

6.6 Where consent is required from SOCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the SOCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the SOCA.

6.7 All disclosure reports referred to the MLRO and reports made to the SOCA will be retained by the MLRO in a confidential file kept for that purpose, for a minimum of six years.

7.0 CLIENT IDENTIFICATION AND DUE DILIGENCE

- 7.1 Due diligence is performed at the account opening stage and where necessary at the after sales stage where a claim or refund is involved. All Individual clients have to provide basic information including name, address, age and occupation. Corporate clients are required to provide lists of their employee policyholders and their dependants (if they are to be covered) including their names, dates of birth and addresses.
- 7.2 Client identification/due diligence is undertaken direct by InterGlobal in respect of its direct individual clients and direct corporate clients in accordance with internal criteria set down for Money Laundering checks. Additional checks are undertaken for transactions falling under the following criteria:
- a) For a business or corporate entity, the nature of a client's business is designated a 'high risk' business. For example, businesses such as Bureaux de Changes or Gambling operations will require a higher level of CDD checks;
 - b) for individuals, a politically exposed person (PEP) and persons connected to them (Connected Persons) such as family members will require a higher level of CDD;
 - c) Clients located in higher risk geographic locations such as areas of known or suspected terrorist financing, arms dealing or areas where Bank of England and OFAC Sanctions apply in relation to specific individuals, business areas or countries, will require higher level of CDD checks;
 - d) Transactions transcending specific internal guidelines depending on whether the client is an individual or a business; transactions that are unusual for the client or unusual requests or highly complex transactions or payment arrangements will require a higher level of Due Diligence.
- 7.3 Non-direct clients i.e. clients that have been introduced by Intermediary. Terms of Business Agreements are held with intermediaries requiring them to comply with all relevant laws applicable to them including conducting customer due diligence on clients. Intermediaries are required to go through an application process and be approved by InterGlobal to introduce business to it. The intermediary is responsible for making the necessary checks. However, clients introduced by intermediaries will be required to undergo further due diligence if they fall into the higher risk category.
- 7.4 Clients purchasing cover through locally licensed insurers in jurisdictions where InterGlobal uses such insurers (fronting insurers): The insurers are responsible for conducting due diligence on the clients. However, if InterGlobal is administering the policy or the claims, then InterGlobal will conduct checks as set out above prior to setting up clients on its systems.
- 7.5 Corporate clients are required to have a designated contact point to reduce the likelihood of receiving instructions from individuals who are not known by the company and to reduce fraud.
- 7.6 Evidence of checks is retained for at least six (6) years from the end of the business relationship or transaction(s).
- 7.7 If satisfactory evidence of identity is not obtained at the outset where this is required, then the business relationship should not proceed.

8.0 MONITORING AND OPERATIONS

- 8.1 A weekly IT sweep of the company's database, Actisure, is performed against the Bank of England Treasury Site's Investment ban and Sanctions lists for any matches. This is monitored by the Compliance function.
- 8.2 Client Services, Credit Control and the Account opening sections of the business use checklists to ensure that all clients are checked at various stages pre and post sales depending on the transaction. The process is reviewed by Compliance.