PIONEER INSURANCE & REINSURANCE BROKERS PRIVATE LIMITED

# FINANCIAL CRIME POLICY

# 2017

Pioneer Insurance & Reinsurance Brokers Pvt. Ltd.
Compliance Officer: Mr. Sanjay Kabra
1219, Maker Chamber V, Nariman Point,
Mumbai, Maharashtra - 400021
INDIA

## 1. INTRODUCTION

We aim to maintain the highest standards of business ethics, honesty, openness and accountability. This policy statement strictly outlines our approach to financial crime. We promote integrity and honesty and do not abide to misdeeds such as Fraud, Dishonesty, Deception, False accounting, Theft, Concealment, Money laundering, Terrorist financing, Corruption, Bribery, including the giving, promising, offering, requesting, agreeing to receive or acceptance of bribes, Market abuse or any other illegal behaviour.

## 2. OBJECTIVE

We aim to:

- Minimise the potential and actual incidence of financial crime
- Detect and report financial crime
- Minimise the risk of resultant losses
- Improve the chance and scale of recoveries
- Make it clear we will not tolerate financial crime
- Promote honesty
- Reduce the opportunities for financial crime in co-operation with other organisations.

## 3. RESPONSIBILITY

The Compliance Officer is the individual in charge for this policy

## 4. SCOPE

This policy applies to all the firm's activities in all territories or jurisdictions in which they are carried out.

## 5. REVIEW

This policy is reviewed and if necessary amended at least every 12 months, to take account of any new regulatory requirements, the changing risk landscape and our performance in preventing and identifying financial crime.

## 6. RISK ASSESSMENT

We assess the financial crime risks to which our business is exposed through analysis of:

- Our customer base: whether we have customers who pose particular risks due to their country of residence, occupation or culture.
- The nature of the business that we seek: whether we are involved in areas of business that are associated with a higher risk of financial crime.
- Our staff – this considers our recruitment practices; training & competency requirements, remuneration policy and whether there are individuals are considered to be a higher risk due to their particular job functions.
- Third parties: the risks posed by third parties and suppliers, including IT suppliers, contractors etc.
- Systems and Controls: the adequacy of our systems and controls in minimising the potential risks of financial crime. This will be identified through the analysis of our customer base, nature of business, staff and third parties. It will include an analysis of physical security and, in particular, security of customer data.

The risks in these areas are to be subject to reassessment at least every 12 months.

## 7. SYSTEMS AND CONTROLS

We will develop and maintain effective systems and controls in relation to:

### 7.1 CUSTOMER IDENTIFICATION

- Verify the identity of our customers
- Verify the identity of any additional parties (e.g. third parties, attorneys, relevant parties to a trust).

Where verification of identity is required and cannot be completed, we may not be able to proceed with the relationship/transaction. We will consider alternative forms of verification, if somebody has a

legitimate reason for not being able to provide the standard forms of evidence of identity.

### 7.2 TRANSACTION SCRUTINY

The Company has a duty to report any suspicion of Money Laundering falling under specific the rules and guidelines. Areas of vulnerability and factors which may give rise to suspicion include:

- A client who wants to pay a large premium in cash
- A request to insure goods in transit to, or situated in, countries where terrorism, the production of drugs, drug trafficking or any general organised criminal activity may be prevalent
- A client who shows little interest in the terms of the policy, or suggests that cost is not an issue, but is more interested in the return premium if the policy is cancelled
- Situations where a client wishes to insure assets well in excess of the client's lifestyle or occupation
- Early cancellation of a policy in circumstances which seem unusual or for no apparent reason
- Cancellation of a policy and a request that the refund be paid to a third party
- Overseas business emanating from countries which may have ineffective or no money laundering legislation or where the rules are not properly enforced

### 7.3 FRAUD DETECTION

Fraud comprises both the use of deception to obtain an unjust or illegal financial advantage and intentional misrepresentations by one or more individuals among management, staff or third parties. All managers, supervisors and staff have a duty to familiarise themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert for any indications of irregularity. These include but are not limited to:

- Theft of Company property, including information;
- Forgery or alterations of Company documents;
- Wilful destruction of Company records;
- Falsification of expenses claims;
- Unauthorised disclosure of confidential information to outside parties;
- Misappropriation or use of Company assets for personal gain;
- Paying fictitious bills or invoices;
- Placing bogus employees on the payroll;
- Unauthorised premium discounting;
- Knowingly generating or paying false claims or invoices;
- Using Company credit cards for personal expenditure.

### 7.4 SUSPECTED OR ACTUAL FINANCIAL CRIME

Our staff members are required to report any knowledge or suspicion of financial crime to the Compliance Officer, who will arrange an investigation. Where appropriate, their concern(s) will be reported to the relevant law enforcement and/or regulatory authorities.

### 7.5 RECRUITMENT

For new employees we always seek references from previous employers. For individuals in financial and data-sensitive areas we will carry out additional background checks, such as criminal records checks and credit checks. The same principles apply to temporary/agency staff and contractors, where we will carry out appropriate due diligence on the organisation concerned, to seek assurances and evidence that similar checks are carried out by the organisations that sponsor or employ such individuals.

### 7.6 THIRD PARTY ORGANISATIONS

A 'third party' is defined as any company or individual who is not the insurer/underwriter or the insured. For organisations that we do plan to do business with (e.g. introducers, suppliers, IT consultants, outsourcers) we will assess the risks of financial crime and carry out due diligence on the organisation concerned, as deemed appropriate to the assessed level of risk. Wherever necessary, we ensure that a contract or terms of business agreement is put in place with provisions that support and reflect our approach to the prevention of financial crime.

All third party relationships will be reviewed periodically. This will include re-visiting and verifying any due diligence previously carried out. If a third party relationship is terminated, the Finance Team must be advised and the records must be updated to show that the relationship has been terminated.

### 7.7 TRAINING & COMPETENCE

All staff members receive relevant and regular anti-financial crime training, which includes competence testing.

### 7.8 WHISTLE BLOWING

All staff members are encouraged to report any suspicious activities, breaches of rules or procedures by colleagues that they identify during the course of their daily activities.

### 7.9 PHYSICAL SECURITY

We ensure a secure working environment with controlled access at all times, with an appropriately higher level of security for sensitive areas such as server rooms and client records.

### 7.10 DATA SECURITY

We ensure to maintain a high level of security in respect of all personal data held on our electronic and other records through:

- Robust, secret and individual passwords for access to systems with mandatory password change on a frequent basis
- Individual system profiles that permit access to only the data needed by the job holder
- Encryption of all electronic data that is removed from company premises
- Controls and monitoring on the use of email/internet and portable data storage/processing devices
- Prompt destruction of credit/debit card information once it has been used
- Maintain a clear desk policy (all hard copy documents containing personal data are to be locked away when the office is closed)
- Secure destruction of IT hardware and client records that are no longer required

### 7.11 BRIBERY AND CORRUPTION

Each member of staff is under an obligation to support the company's regulatory responsibilities regarding anti-bribery and corruption. This includes assisting the Company in identifying, mitigating and preventing the risk of illicit payments or inducements to third parties. A 'third party' is any company or individual who is not the insurer/underwriter or the insured.

Payments and inducements can include, but are not limited to:

- one-off payments
- commissions (initial and/or ongoing)
- excessive entertainment
- gifts and hospitality and the provision of "free" personal insurance.

We will monitor all expenses claims to identify expenditure on client entertainment/gifts with any expenditure. Payments must be clear and justified in relation to the work done. We will monitor commission and all other payments to third parties to identify any payments which are unusual or not as expected. Decisions will be made by after a case for making the payment is put by the account handler or the account executive/director. The reasoning behind any payments must be documented and, where necessary, supported by the completion of a Third Party Due Diligence Enquiry form.

### 7.12 MANAGEMENT INFORMATION

We ensure to develop and maintain Management Information systems that are able to monitor the effectiveness of all the above systems and controls. The output of this MIS will be reviewed on a regular basis by the senior management team, who will report unusual activities and adverse trends to the Board.