Fraud, Bribery & Money Laundering Policy

PHX092

Contents

Phoenix Software is committed to the highest ethical standards and is culturally aware of the prevention and detection of fraud, bribery, money laundering and financial crime including theft (hereon in collectively referred to as "Financial Crime") and will uphold all relevant UK legislation. It requires its employees and any person working on behalf of the Company to act at all times with honesty, integrity, propriety, and due care in all matters, but particularly in the safeguarding of the Company, its associated assets, its reputation, and that of its organisational group.

The Company has a zero-tolerance approach to Financial Crime or any other form of corrupt behaviour and actively encourages anyone working with the business as an employee, contractor, client, or partner, to report breaches in procedures to the Company's Managing Director immediately. All reports will be dealt with in a safe and confidential manner (see 'Whistleblowing Policy') and will be investigated rigorously. Any breach of this Policy by a staff member may ultimately lead to dismissal via the Company's disciplinary procedure.

The purpose of this Policy is to set out individual responsibilities with regards to the prevention of, detection of and response to Financial Crime including what to do in the event of a suspected offence and what action will be taken by the Company in the event that an offence has been committed. The Policy is based on five key principles:

- **Principle 1:** It is based on risk and has been written to convey to employees the expectations of the Board regarding managing such risks.
- **Principle 2:** The risk exposure which is assessed by the Board to identify specific potential events that it needs to mitigate.
- **Principle 3:** Prevention techniques and controls to avoid potential risk events are established, where feasible, to mitigate potential impacts to the Company.
- **Principle 4:** Detection methods and controls are established to uncover risk events when preventative measures fail, or unmitigated risks are realised.
- **Principle 5:** A response process, including reporting, is in place to solicit inputs on potential risk events and a coordinated investigation approach is used to ensure potential offences are dealt with in a timely manner.

Who Is Affected By This Policy?

This Policy applies to the Company and all other parties who are given access to the Company's information and premises.

This Policy covers all persons whether:

- Employees of the Company
- Board/committee members of the Company
- Temporary agency staff or volunteers
- Consultants, contractors, and agents (whether employed on a casual or freelance basis or otherwise)

If the action taken by the Company includes disciplinary action in relation to a member of staff, the Company's disciplinary policy and procedure is followed.

Fraud

The Fraud Act 2006 broadly defines three main types of fraud:

- **Fraud by false representation** - where an individual dishonestly and knowingly makes a representation that is untrue or misleading.
- **Fraud by wrongfully failing to disclose information** - where an individual wrongfully and dishonestly fails to disclose information to another person when they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose it, or they would be reasonably expected to disclose it.
- **Fraud by abuse of position** - where an individual who has been given a position in which they are expected to safeguard another person's financial interests dishonestly and secretly abuses that position of trust without the other person's knowledge.

The Act also includes offences of obtaining services dishonestly and of possessing, making, and supplying articles for use in frauds, and of fraudulent trading applicable to non-corporate traders.

For fraud to be committed under the legislation there will need to be an identifiable intent by the individual to make a gain or to cause a loss or to expose another to the risk of loss.

The Fraud Act 2006 does not apply in Scotland, where fraud is a common law crime and offences include "falsehood, fraud and wilful imposition". For the avoidance of doubt however, this Policy applies in full to Scotland.

Examples of fraud

Some examples of actions that could be considered to be fraud are as follows, although the list is by no means exhaustive:

- Theft of any company property
- Theft of petty cash / banking's
- Forgery or alteration of any document, for example a cheque
- Destruction or removal of records
- Falsifying expense claims
- Receiving incorrect salary overpayments and not informing or re-imbursing the Company
- Use of the Company's assets and facilities for personal use
- Fraudulent use of computer time and resources, including unauthorised personal browsing on the Internet

These last two examples would obviously exclude any reasonable, occasional but limited personal use, for example phone calls when away on company business or personal use of the computer in accordance with the Company's Acceptable Use Policy.

Bribery

Definitions/offences of bribery

- **Active Bribery** - offering, promising, or giving bribes
- **Passive Bribery** - requesting, agreeing to receive, or accepting bribes
- Failure of a commercial organisation to prevent bribery

Examples of Bribery

- Allocation of property without following approved allocations policies and procedures, in return for a reward
- Offering employment without following approved recruitment policies and procedures, in return for a reward
- Acceptance of gifts, goods and/or services as an inducement to giving work to any supplier
- Disclosing confidential information to outside parties without authority for personal gain

* Unacceptable gifts include those that:

- Are illegal or involve a biased or dishonest act
- Would result in the violation of any law
- Involve conduct of a sexual nature and/or violation of mutual respect
- Create mutual agreements (requiring anything in return for the gift)
- Violate the Company Corporate Code of Conduct (See Gift Register guidelines)

Money Laundering

The Company mitigates money laundering risks effectively through:

- identifying our customers and knowing their ownership and control structure
- understanding our relationship with them

Internal controls and monitoring systems are in place to alert staff should criminals try to use the Company for money laundering, try to purchase goods fraudulently or to engage in any other Financial Crime.

Once aware of any potential threat, the Company will take steps to prevent it and report any suspicious activity to the National Crime Agency.

The Company is constantly vigilant to new types of Financial Crime and constantly looks to amend its control environment where necessary to respond to new threats.

Examples of money laundering activity

- Sudden changes in customer ordering, delivery and/or payment requests, or those who may agree to bear very high or uncommercial penalties or charges
- Other irregularities and/or suspicious transactions both within the Company and in organisations with which the Company contracts with

Managing the Risk – A Risk-Based Approach

Financial Crime should be considered as a set of risks to be managed alongside other business risks and, therefore, needs to be embedded into the Company's risk management process. It combines the likelihood of the offence occurring and the corresponding impact measured in monetary, legislatory, customer/client or reputational terms.

Preventative controls and the right type of culture operating within the Company will reduce the likelihood of Financial Crime occurring while detective controls and effective contingency planning can reduce the size of any losses or damage to the Company's reputation.

In broad terms managing the risk involves:

- Assessing the Company's overall vulnerability to Financial Crime
- Identifying the key risk areas most vulnerable to the risk
- Considering the likely impact of an offence occurring in these key risk areas
- Assessing the scale/likelihood of an offence occurring in the key risk areas
- Identifying and evaluating existing controls to prevent an offence
- Developing an action plan and assigning ownership
- Implementing revised controls to improve the Company's approach
- Reviewing, monitoring, and evaluating the impact of revised controls
- Measuring the effectiveness of the risk-based approach

Managing the risk of Financial Crime is the same in principle as managing any other business risk and the annual risk management cycle should, therefore, look to cover areas set out below:

Identifying the key risk areas

The Board should:

- establish the areas most vulnerable through the responsible managers undertaking an overall review of their local areas of activity to identify those areas most vulnerable to Financial Crime, for example, cash handling, procurement, accounts payable, allocations, recruitment, asset protection and sensitive information.
- identify patterns of loss, if applicable, and areas of potential loss so that vulnerable areas can be pinpointed.

Considering the impact

Managers assess the possible impact that any type of reported crime can have in a wide variety of areas including, for example:

- the overall reputation of the Company
- potential financial loss
- loss of confidence in the organisation
- effect on staff morale and productivity
- potential increase in insurance costs
- need to utilise resources in investigative work

Assessing the scale/likelihood

Managers assess the possible scales and likelihood of Financial Crime as well as counter-arrangements in place. This analysis considers:

- the impact of potential Financial Crime both on the organisation corporately and in relation to the specific operational area
- monitoring and review of national/local trends in relation to new and emerging Financial Crime and considering the potential impact on the Company

Identifying the adequacy of existing controls

Managers evaluate the adequacy of existing controls and establish what further controls or enhancements to existing controls are required to mitigate the risk. An element of proportionality is used when considering the extent and cost of suggested improvements to control measures.

- Adequate segregation of duties between key control areas
- Staff resources that are sufficient to provide adequate control and are organised in a structured manner
- Published local schemes of delegation identifying levels of responsibility and authority
- Regular reconciliation of budgets that are subject to independent review
- IT security arrangements (including security systems and codes of conduct for IT usage)
- Asset control register (cash, fixed assets), inventories, asset marking, etc.
- Documented policies and procedures that are subject to regular review
- Maintenance of adequate records of risk assessment procedures

Prevention and Detection

The Company has in place a framework of preventative measures, including internal controls, designed to prevent Financial Crime occurring in the first instance.

These consist of rules, regulations, policies and procedures within which employees, board/committee members, agency staff, consultants and contractors are expected to operate and include:

- A Code of Conduct
- Disciplinary procedures for employees
- A Whistleblowing Policy
- Financial Principles and Regulations
- Gift Register

It is the responsibility of managers to actively deter, prevent and detect Financial Crime by maintaining good control systems and ensuring that their staff are familiar with them.

The most common control weaknesses that management should be aware of include:

- Too much trust being placed in employees
- Lack of proper procedures for authorisation
- Lack of adequate segregation of duties
- Lack of independent checks on employee activities
- Lack of clear line of authority
- Infrequent reviews of departmental authority
- Inadequate documents and records (leading to a loss of a 'management trail')

Prevention is preferable to detection therefore preventative controls should be applied as appropriate, bearing in mind, the risk of Financial Crime and the potential for loss to the Company. Preventative controls may not be sufficient however, to guard against determined individuals and detective controls are therefore important. Detective controls are established to detect errors, omissions and Financial Crime after the event has taken place.

Preventative and detective controls (PC and DC) include but are not restricted to:

- Physical security (PC)
- Logical (computer) access security (PC)
- Organisational (PC)
- Supervision and checking of outputs (PC & DC)
- Management trail (DC)
- Monitoring (PC & DC)
- Asset accounting (DC)
- Budgetary and other financial controls (DC)
- Systems development (PC & DC)
- Staffing (PC)

Management are alerted to the factors which might indicate that Financial Crime is taking place.

These include:

- Opportunity (e.g. where there is a lack of separation of duties so that one person has control over all aspects of a transaction, for example, over a purchase order, purchase invoice and purchase payment authorisation).
- Over-ride (e.g. where a manager over-rides the normal control system/procedure. In practice this may be necessary, however, if done frequently it may be indicative of non-compliance).
- Situational pressure (e.g. personal factors, which may be indicative of a tendency / temptation to Financial Crime).

Staff need to be vigilant to the warning signs and indicators of Financial Crime.

Financial Crime Prevention: Risk Register

It is the responsibility of Senior Management to assess and review the risk of Financial Crime in their area and to ensure that local line management and colleagues implement any action plans.

Related Documents

Please also read:

- Anti-Tax Evasion Policy
- Whistleblowing Policy
- Gift Register Guidelines

Version Control

Author	Version	Date	Description
Trevor Hutchinson	1.0	01/09/2019	Original Document
Trevor Hutchinson	2.0	01/09/2020	Amendments following annual review
Trevor Hutchinson	3.0	01/11/2021	Amendments following annual review
Trevor Hutchinson	3.0	01/11/2022	Annual review – no changes

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/09/2019	Managing Director
Sam Mudd	2.0	01/09/2020	Managing Director
Sam Mudd	3.0	01/11/2021	Managing Director
Clare Metcalfe	3.0	01/11/2022	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 01/11/2022