FSPAML18

Design and monitor an internal reporting system for suspicious transactions and activities

Overview

This standard is about developing a system in your organisation for identifying and reporting suspicious transactions and activities, which is likely to take the form of a suspicious activity report (SAR). You must ensure staff appreciate the mandatory need for reporting suspicious transactions and activities and the impact on the overall health of your organisation.

You must deal with reports about suspicious transactions, analysing them and determining the need for further action, and you need to keep secure records of all relevant information and of the evaluation process.

Your system must ensure that 'tipping off' does not occur.

Performance criteria

You must be able to:

1. identify the reporting lines for suspicious transactions and activities 2. design a system which will provide adequate evidence that a suspicious transaction or activity has been reported, whilst balancing the need to discourage frivolous or irresponsible reporting 3. implement a process in the reporting system to ensure that enquiries into clients do not result in 'tipping off' 4. inform all staff they must raise a SAR whenever they suspect criminal activity in a transaction, reminding them of the continuing legal obligations with regard to the client concerned and addressing any awareness issues that arise 5. deal promptly with internal reports of suspicious activity received from staff, determining if the report needs further investigation 6. discuss the report with relevant internal colleagues and managers to elicit further information required to make a decision 7. decide whether or not to internally escalate or externalise the report taking into account the level of suspicion, validity any malicious intent and any other relevant factors 8. monitor any further dealings with the subject of the report to determine whether further reports are required 9. keep accurate, confidential and secure records of the evaluation process which include all relevant information relating to the report 10. provide information on the number of reports into suspicious transactions and activities made by staff, and from which parts of the organisation they originate 11. monitor and regularly review the operation of reporting systems to identify trends, issues and problems and areas for improvement 12. adapt and modify the reporting system and process as required 13. provide feedback to relevant staff on the decisions regarding the report into suspected suspicious transactions and activities, as appropriate

Knowledge and understanding

You need to know and understand:

1. reporting lines for staff 2. definitions of the subjective and objective tests of suspicion and the importance of these, including how suspicion differs from speculation and that proof of crime is not required 3. difference between defensive and mandatory reporting of suspicions and when each is required 4. what constitutes knowledge for the purposes of the criminal offence of Money Laundering and Terrorist Financing 5. how to encourage responsible reporting of suspicious transactions and activities, and how to discourage frivolous reporting 6. strengths and weaknesses of suspicion-recognition systems 7. how to evaluate internal reports of suspicious transactions and activities, determining if the report has merit and should be externalised 8. how to evaluate reports to determine any malicious intent 9. documentation required by your organisation and by external enforcement authorities of your evaluations of internal reports 10. why the reports and your evaluation of them must be stored securely 11. how to manage communications with clients who are suspected of Money Laundering or Terrorist Financing, and their advisers 12. how to handle the risk of committing the 'tipping off' offence 13. the purpose of monitoring and reviewing the reporting system 14. how to identify improvements to the reporting system 15. your organisation's requirements relating to the application of codes, laws regulatory requirements and guidance, and potential conflicts with other regulatory regimes, as they impact on your activities

Glossary

Anti-money laundering and counter terrorist financing measures
This encompasses all required policies, procedures and systems as well as the requirement for regulated organisations to apply enhanced customer due diligence and enhanced ongoing monitoring on a risk-sensitive basis in certain defined situations and any other situations which present a higher risk of Money Laundering or Terrorist Financing.

Relevant authorities
This should be extended to all jurisdictions which have control over the organisations, including regulatory, statutory, legal, investing, licensing, issuing and supervisory authorities.

Staff
Staff includes all levels and categories, including contractors, suppliers, temporary workers and interns.

FSPAML18

Design and monitor an internal reporting system for suspicious transactions and activities

Developed by	Skills for Justice
Version Number	2
Date Approved	31 Jan 2016
Indicative Review Date	31 Jan 2021
Validity	Current
Status	Original
Originating Organisation	Financial Skills Partnership
Original URN	FSPAML18
Relevant Occupations	Finance, Financial Institution and Office Managers, Financial Institution Managers
Suite	Anti-money Laundering
Keywords	Anti-money Laundering; Countering Terrorist Financing; reporting systems; suspicious transactions