Financial Crime Policy

Master List Ref	Release Date	Review Date	Next Review Date
COM001	August 2015	January 2026	April 2026
Version:	**Process Owner**	**Reviewed by**	**Approved by**
5.2	Legal & Compliance	Associate Director Compliance	AVP Legal

Table of Contents

1. Introduction

The 'Financial Crime Policy', hereinafter, referred to as "Policy" or "Policies and Procedures" is applicable for UK operations and any operations globally whereby UK clients or UK transactions are undertaken.

2. Scope

These Policies and Procedures apply to all Firstsource UK employees, whether permanent, on contract or temporary, consultants or secondees along with any contractors and clients working with Firstsource and suppliers of Firstsource. In addition, UK clients based outside out of the UK and any employees dealing with UK clients globally must adhere to this policy.

In light of the potential penalties and possible reputational damage to both Firstsource and their clients; all employees and contractors have an obligation to comply with this policy. Breaches of this Policy will be taken seriously and could result in action being taken under the Firstsource disciplinary procedure against employees and the termination of any contractor relationships for material breach.

The purpose of this policy is to protect the brand, reputation and assets of Firstsource and its clients from loss or damage resulting from potential and/or suspected incidents of financial crime; in addition to safeguarding the confidentiality of client and customer data used for providing services to our clients.

The policy aims to achieve the following objectives:

- Promote zero tolerance to financial crime.
- Spread awareness and educate employees on financial crime risks faced by Firstsource.
- Encourage all employees / associates of Firstsource to report cases of financial crime.
- Identify and address organisation vulnerabilities through proactive and reactive measures

3. Risks

This policy aims to significantly reduce the risk of:

- Firstsource or its customers suffering financial loss and/or being the victim of, or facilitating the perpetration of acts of money laundering, terrorist financing, internal or external fraud, bribery

and corruption, or breaching international financial or economic sanctions.

- Regulatory censure and/or fines against Firstsource due to inadequate processes and controls.

4. Applicability of the policy to third-party suppliers

The circumstances in which the policy would be applicable to the third-party supplier of goods and services to Firstsource are:

- On-boarding or introducing customers.
- Processing customer transactions.
- Providing Firstsource's financial products to customers.
- Providing risk, compliance or audit services to the Group.

The circumstances in which the Policy would not be applicable to the third-party supplier of goods and services to Firstsource are:

- Providing goods to Firstsource.
- Performing services unrelated to Firstsource's regulated activities (e.g. security, transport, catering, printing etc).
- Conducting activities outside the scope of Regulation 3 of the UK Money Laundering Regulation 2007 (or equivalent).

Whilst every effort has been made to ensure that this list encompasses as many scenarios as possible the list is not exhaustive – if you are unsure or have any queries please contact the Legal and Compliance team at ukcompliance@firstsource.com and they will be happy to answer any queries you may have.

5. Third party acceptance policy

Prior to Firstsource UK initiating contracts with any third parties, a background verification check is undertaken to ensure we are only working with suppliers we deem acceptable. This is based on the outcome of their checks and the assurance this provides that the relationship will not be detrimental

to Firstsource's regulatory obligations and to deliver our services in an ethical and transparent manner. These checks include:

- Government/Political Relationships.
- Bribery, corruption and fraud.
- Criminal/illegal activities.
- Financial concerns.
- Regulatory non-compliance.
- Litigation.
- Adverse media and other concerns.

6. Board statement

Firstsource is required by law to implement procedures geared to combating Financial Crime. Failure to do this can result in fines and/or imprisonment for the Senior Manager/Director(s) responsible. However, all staff are responsible for understanding their obligations and complying with the policies and procedures in place to combat Financial Crime. In order to document their commitment to their obligations the Board has issued the following statement.

"The Board takes its obligations regarding Financial Crime very seriously. It will aim to ensure that the necessary processes and procedures are in place in order to fulfil its legal and regulatory obligations and has a zero tolerance for failure and breaches. In order to achieve this outcome, it will endeavour to achieve best practice and the highest possible standard of competence by putting the following in place:

- Appointing a suitably competent Money Laundering Reporting Officer (MLRO) to oversee the AML Compliance Program.
- Ensuring that money laundering is discussed, at least quarterly within Board meetings; or more frequently should the need arise or an issue highlighted.
- Ensuring staff have access to Financial Crime training, on an annual basis as a minimum.
- To ensure that an AML compliance program is put in place along with procedures, support and guidelines which includes customer due diligence and monitoring measures in line with AML regulations.

- Co-operating fully with relevant agencies.
- Ensuring that all relevant records are kept secure.
- Ensuring financial crime is considered when considering new products or business activities".

7. Training

The Proceeds of Crime Act 2002 states that the absence of adequate training by an employer, as required by the regulations, will provide a defense for staff against a criminal charge of not reporting knowledge or suspicion of money laundering. The defense is not available where a member of staff would have had reasonable grounds to suspect that money laundering was taking place.

A successful defence, on the part of a member of staff of not having been trained to recognise and report suspicions will leave the Company itself liable to prosecution for breach of the Regulations. It is therefore, important that training for relevant staff is made compulsory and that an appropriate record thereof is maintained. This compulsory training for relevant staff is mandatory upon induction and at least annually thereafter.

8. Timing and approach to training

Training is provided in three ways:

- Training on induction by both the Client (where applicable) and Firstsource;
- Annual Training by both Client (where applicable) and Firstsource;
- Ad hoc training, carried out by the Client, on an individual basis for those members of staff whose roles require an in-depth knowledge of Financial Crime.

A record of all training will be maintained by the training team with completion reports circulated on a weekly basis to any relevant individuals who are required to monitor completion rates.

Staff are reminded if they have any queries or are unsure of their obligations under any policies to discuss with either their line managers or to contact Legal and Compliance on ukcompliance@firstsource.com.

9. Background to financial crime within the legal

and regulatory regime

Firstsource, as a solo regulated firm is required to comply with the Financial Conduct Authority's requirements to have systems and controls in place to mitigate the risk that we might be used to commit financial crime; and, as a company within the financial services sector we also have obligations to comply with the following acts and regulations placed on us by law:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
- The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.
- The Proceeds of Crime Act 2002.
- The Terrorism Act 2006.
- Bribery Act 2010.
- Fraud Act 2006.
- All relevant Joint Money Laundering Steering Group guidance.
- FCA SYSC requirements.
- Sanctions and Anti-Money Laundering Act 2018.

10. The Financial Conduct Authority (FCA)

The Financial Conduct Authority is the UK's main financial services regulator with authority over banks, building societies, credit unions and other firms engaging in financial activities. The FCA oversees compliance with AML regulations in the UK and has the power to investigate money laundering and terrorism financing offenses in conjunction with other law enforcement agencies and authorities The Financial Conduct Authority has three main objectives, which are:

- To protect consumers from bad conduct.
- To protect the integrity of the UK financial system.
- To promote effective competition in the interests of consumers.

In order to achieve the above the FCA expects each company to:

- Have a thorough understanding of its financial crime risks in order to apply proportionate systems and controls.

- Have an organisational structure that promotes coordination and information sharing across the business.
- Have appropriate up-to-date policies and procedures in place that can be easily accessed and understood by all staff.
- Employ staff who have the skills and expertise to do their jobs effectively.
- Review employees' competence and take appropriate action to ensure they remain competent for their role.
- Manage the risk of staff being rewarded for taking unacceptable financial crime risks.
- Be able to provide evidence to demonstrate that it has adequate systems and controls to prevent the risk that it might be used to further financial crime.

The FCA also expects all systems and controls to be subject to challenge. Senior management must therefore ensure that robust testing, auditing and compliance is in place to routinely test the defence against financial crime and report and remediate where there are deficiencies.

11. The Joint Money Laundering Steering Group (JMLSG)

The joint Money Laundering Steering Group is made up of the leading UK Trade Association in the Financial Services Industry. Its aim is to propagate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance.

The guidance sets out what is expected of firms and their staff in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements, taking into account the particular circumstances of the firm, and its products, services, transactions and customers.

A copy of the current guidance can be found here: https://jmlsg.org.uk/guidance/current-guidance/

12. Money laundering

Money Laundering is the process by which criminals take the money they have gained from illegal activity and seek to give it the appearance of legitimacy, hence the term 'money laundering'.

Money Launderers often undertake a number of transactions to conceal the original source. The term money laundering can be used to describe money derived from any criminal activity - not just drugs or terrorism. Any activity, which would be a criminal offence, if committed in the UK, is classed as “serious criminal conduct”, wherever in the world it is committed. Any money related to serious criminal conduct is subject to the Money Laundering Regulations.

The term “Laundering” is used as the money derived by the criminals is described as “dirty”. However, once it has been successfully laundered it appears to be “clean” and free from any suspicion. The United Nations Office on Drugs and Crime estimate that between £634 billion and £1.59 trillion of money is laundered globally each year.

The Proceeds of Crime Act (POCA) defines Money Laundering as an offence which includes all forms of handling or possessing any criminal property, including possessing the proceeds of one's own crime, and facilitating any handling or possession of criminal property. Money laundering covers all the areas below and more:

- People trafficking.
- Terrorist financing.
- Benefit frauds.
- Drug dealing.
- Tax evasion.
- Market abuse and insider trading.

This list is not exhaustive.

13. Financing or facilitating terrorism

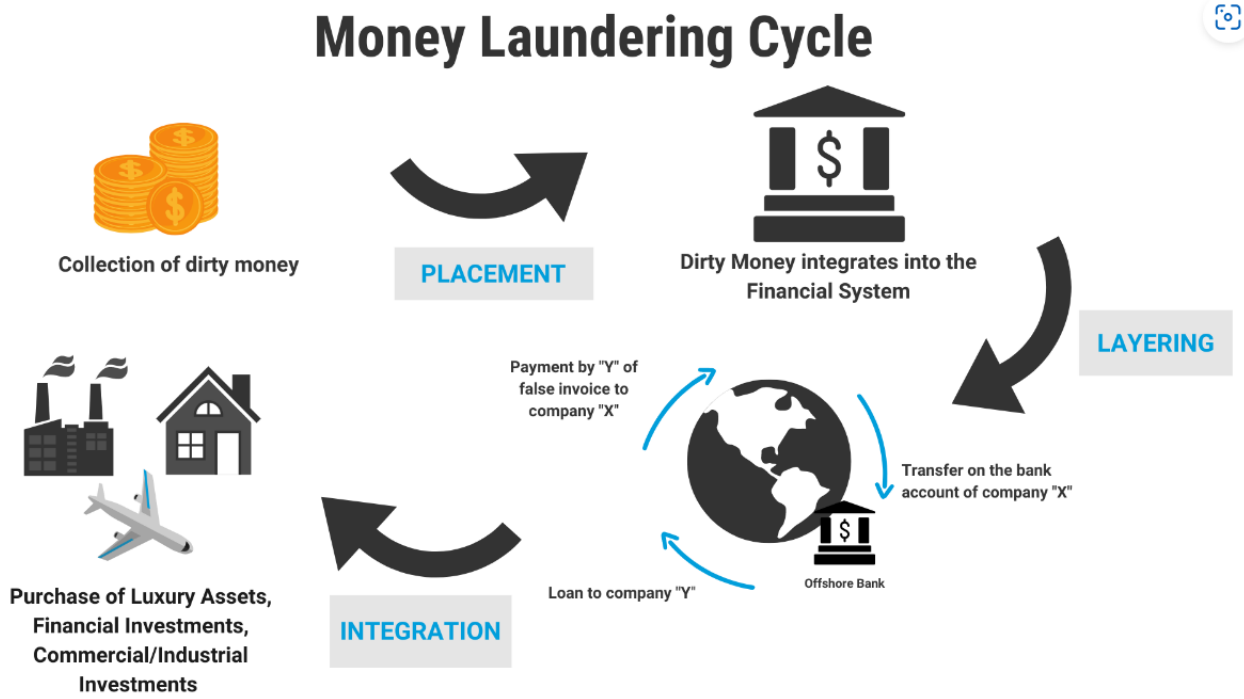
It is a criminal offence to finance or facilitate the financing of terrorism, and there are legal obligations under the Prevention of Corruption Act, 2002 to submit suspicious activity reports when we suspect criminal activity. We have therefore implemented procedures to prevent us being used by money launderers or for terrorist financing. We supply training and guidance to all staff to ensure they are aware of the laws designed to prevent money laundering and terrorist financing and our procedures for doing so. If any member of staff suspects criminal activity they should file a Suspicious Activity Report or contact the Compliance and Legal team on ukcompliance@firstsource.com .

Firstsource takes its obligations regarding financing of terrorism very seriously. As such the Legal and Compliance team will keep and monitor a ‘SAR risk register’ as and when required to review any reported activities and to mitigate any risks or patterns should they occur.

Due to the confidential nature of SAR reporting the SAR risk register will only be accessible by the Legal and Compliance team.

14. How money is laundered

Money laundering is the process by which the identity of "dirty money" (i.e. the proceeds of criminal activity) is changed so that it appears to come from a "clean" source. This includes the proceeds of all crimes and not just those involving serious crime.



Source - Overview (unodc.org)

Money being laundered will typically go through three stages:

Placement.

The physical disposal of cash, either through banks or other financial institutions, or the purchase of large expensive items.

Layering.

The point at which the funds are disguised and an attempt is made to create a certain amount of distance from the original point of entry into the financial system. At this point there will be an

attempt to confuse the audit trail by carrying out lots of transactions, including investment in legitimate businesses and the resale of high value goods. This can involve several transactions designed to confuse the trail. The idea is to conceal the origin of the money by moving it around the world, using several different financial institutions, and putting as many steps or “layers” in as possible. Assets can be bought and sold, an example of this is a yacht or plane, which is bought in one country, sailed or flown around the world and sold somewhere else.

Integration.

The point at which the money is made to appear more legitimate. Commonly, a company is set up which the over-invoices, or produces false invoices in the company’s name to create an impression that the proceeds are generated from a legitimate source. Purchases of property and other non-cash investments are also used.

The ways of laundering money are becoming increasingly complex and inventive. The more transactions there are in the trail the more difficult it is to trace the money back to its origins.

15. How to identify money laundering

Key questions should be asked to help spot a potential money laundering transaction. These include:

- Who is the customer?
- Is the customer secretive?
- Does the transaction make commercial sense?
- Is the customer or money coming from abroad? Be wary of customers or sources of funds originating from jurisdictions where there are no tight money laundering controls in place? The FATF Blacklist, UK, US and EU Sanction List can be used as reference points for jurisdiction where there are no tight money laundering regulations in place.
- Is there evidence of unsupported customer wealth, both in individual and corporate clients? This should trigger further questions.

Monies received or transferring to one of the countries on the Financial Sanctions list must be reported immediately to the Client, through the procedure you have been given or to the Money Laundering Reporting Officer. The current sanction listed countries at present can be viewed on the UK Government`s website via the following link: The UK Sanctions List - GOV.UK (www.gov.uk).

Additionally, reference should be made to the FAFT Blacklist and OFAC sanctions list which can be viewed via the following links: "Black and grey" lists (fatf-gafi.org) and Sanctions List Search (treas.gov).

Firstsource will not deal with any individuals and/or entities that are sanctioned by the either UK, US or EU sanction restrictions.

16. What to do if you suspect money laundering?

Every member of staff is required to complete a Suspicious Activity Report (SAR) if they know, suspect, or has reasonable grounds to suspect fraud or money laundering and send this to ukcompliance@firstsource.com. A Suspicious Activity Report can be found in Appendix 1.

It will be the responsibility of the Legal and Compliance team to reinforce the message of the importance of recognising and reporting suspicious activities as soon as any employee suspects or becomes aware of such as well as maintaining the SAR risk register.

Failure to report could result in disciplinary action and even result in criminal prosecution. The law imposes personal obligations; these obligations apply to all staff involved in the financial sector. Staff are protected against criminal prosecution once they have submitted their suspicions either to the Money Laundering Reporting Officer, or to the Client as per the agreed process. The Proceeds of Crime Act creates the offences concerning failure to report. An overview of the offences and penalties are provided below.

17. Proceeds of Crime Act 2002 (POCA)

The Proceeds of Crime Act 2002 (POCA) is a UK legislation that addresses the recovery and confiscation of proceeds made from criminal activities and money laundering

18. Reporting obligations under POCA

The reporting obligations in POCA are applicable to anyone in the UK that may interact with an individual or business, whereby they may commit a money laundering offence. Those working in the 'regulated sector' (which includes banks, solicitors, accountants and estate agents) commit an offence if they do not submit a Suspicious Activity Report (SAR) to the Money Laundering Reporting Officer (MLRO) or the Legal and Compliance team on ukcompliance@firstsource.com if they know or suspect, or have reasonable grounds to know or suspect that another individual or person is engaged in money laundering; and the information came to them in the course of their business in supporting regulated clients. A copy of the SAR template can be found at Appendix 1.

Firstsource maintains a SAR risk register and regularly communicates to all employees the importance of staying away of suspicious activity and reporting any suspicious as soon as any

employee suspects any such activity has been committed as part of its compliance framework.

19. Defence against money laundering under POCA

POCA allows someone who reports a potential offence a defence against a money laundering offence by seeking the consent of the MLRO to undertake an activity which the reporter believes may constitute one of the three money laundering offences (i.e. a “prohibited act”). The MLRO will then decide whether to report the suspicion to the National Crime Agency (NCA). Where a suspicion is reported, if the MLRO does not receive a 'refusal to proceed' from NCA within a seven-day period then you can proceed with the transaction.

The legislation covers all criminal property, where the alleged offender knows or suspects the property constitutes or represents benefit from any criminal conduct.

There is a wide definition of "property" and it includes all property situated anywhere in the world

20. Money laundering offences and penalties under POCA

The three principal money laundering offences are contained in sections 327, 328 and 329 of POCA. These offences are punishable by a maximum of 14 years’ imprisonment and/or a fine.

Section 327

An offence is committed if a person conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the proceeds of crime which the person knows or suspects represents the proceeds of crime.

Section 328

An offence is committed when a person enters into or becomes concerned in an arrangement which he knows or suspects will facilitate another person to acquire, retain, use or control criminal property and the person knows or suspects that the property is criminal property.

Section 329

An offence is committed when a person acquires, uses or has possession of property which he knows or suspects represents the proceeds of crime.

In addition, sections 330 and 331 of POCA create an obligation on those persons in the regulated sector to report their suspicion or knowledge of another person’s money laundering to the National

Crime Agency. Failure to report is a criminal offence.

The Money Laundering Reporting Officer or his deputy (the Legal and Compliance team) will always investigate all reports of suspicious activity and where appropriate will submit a report to the National Crime Agency.

Offence
Fail to establish and maintain Money Laundering procedures to guard against being used for this purpose.

Penalty
2 years' imprisonment and/or fine. Proceedings can be taken against Firstsource and the Director(s)/Senior Manager(s) responsible.

Offence
Provide assistance to a Money Launderer if you know, or suspect, criminal conduct. Providing assistance means allowing the Launderer to carry out transactions without reporting them.

Penalty
14 years' imprisonment and/or fine.

Offence
Tip off. This means informing the suspect, or a 3rd party, that a disclosure has been, or is about to be made.

Penalty
Maximum 2 years' imprisonment and/or fine.

Offence
Fail to report if you acquire knowledge, or suspicion, of Money Laundering, in the course of your employment and do not report this as soon as is "reasonably practical".

Penalty
5 years' imprisonment and/or fine.

21. Reporting suspicions of money laundering

All suspicions of money laundering must be reported without delay. They should be discussed in the first instance with your line manager and should also be brought to the attention of the Legal Team at ukcompliance@firstsource.com. Alternatively, you can report it directly to the MLRO. The suspicion should not be discussed with anyone else.

Further, any discrepancies between the information the firm holds on their customers compared with the information held in the Companies House Register must be reported to the Companies House.

Important: Do's

- Report immediately / as soon as you are aware of an alleged incident.
- Provide the following information along with the incident:
  - Who is the suspect (name)?
  - What has the suspect done?
  - Copy of evidences that you may have.
  - Other information like contact details, program / process / department, names of third parties, if any.
  - Your name and contact number, which may be required to get further details, if any.
- Safeguard the original evidence.

Important Don'ts

- Do not delay in reporting the incident. The more you delay, the longer the exposure to the fraud which may mean greater losses to the Company and / or to you.
- Do not hide any information while reporting the incident.
- Do not tamper with any evidence / original documents.
- Do not try to investigate the incident yourself.
- Do not share information with anybody. Process as defined in External Engagement section of External Engagement – Speaking Opportunity Policy to be followed for all communications.

If the Money Laundering Reporting Officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to the NCA. Under POCA, the nominated officer is

required to make a report to the NCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

The NCA prefers that SARs are submitted electronically via the secure internet system SARs Online, or via a dedicated bulk reporting facility. Information about access to and guidance on the use of SARs Online can be found at SAR Portal | Landing page (nationalcrimeagency.gov.uk).

22. Obtaining consent

The Proceeds of Crime Act (POCA) requires firms to obtain consent in order to undertake a transaction where money laundering is known or suspected; or there are reasonable grounds to suspect.

The National Crime Agency (NCA) has seven working days from the first working day after a report is made, to grant or withhold consent to undertake a transaction. If consent is withheld, then there is an additional period of 31 days from the date the MLRO or his deputy is informed consent has been refused. The authorities are required, in this time, to conduct an investigation and where appropriate, serve a court order.

If consent is withheld the Money Laundering Reporting Officer will keep the reportee informed and advise how to deal with the situation without tipping off.

Remember – you must not inform the suspect that a report has been made to either the Money Laundering Reporting Officer or the NCA. This is referred to as 'tipping off' and can carry a maximum penalty of 5 years' imprisonment and/or a fine.

23. Customer due diligence

All members of staff must identify and verify all customers/entities/individuals (including directors and beneficial owners) before entering into a relationship and throughout the lifecycle of the relationship as per policies and procedures provided by Firstsource and/or the Client.

For high Risk Factors, such as;

- Relevant transactions between parties based in high-risk third countries.
- The customer is the beneficiary of a life insurance policy.
- The customer is a third-country national seeking residence rights or citizenship in exchange for Transfers of capital, purchase of property, government bonds or investment in corporate entities.
- Non-face to face business relationships or transactions without certain safeguards.

- Transactions related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or archaeological, historical, cultural and religious significance.

The following procedures shall apply:

- Obtain additional information on the customer and beneficial owners, the intended nature of the business relationship, the source of funds of the customer and the reasons for the intended transactions.
- Carry out enhanced monitoring of any business relationship or transaction involving a high-risk third country, rather than only those established in a high-risk third country.
- Obtain senior management approval before establishing or continuing a relationship involving a high-risk third country. This was previously only required for credit and financial institutions.

24. Transaction monitoring

The words Know Your Customer, in the financial sense, describe the process by which a bank or financial institution checks the identity, background and other aspects of the source of wealth of potential and existing customers. Also known as KYC, legislation and regulation require firms to obtain evidence of identity of a customer at take-on and to keep a record of that evidence for as long as there is a relationship with a customer. Transaction monitoring is completed by the client and in some instances also by the Firstsource onsite quality team by request of the client.

Legislation and regulation also require a firm to keep up to date its knowledge of a customer throughout the life of the relationship, so that changes in the customer's activity can be assessed and dealt with, all with the principal aim of preventing Money Laundering and Financial Crime.

Circumstances which may indicate monitoring should be undertaken are:

- When the customer tries to make a payment from overseas;
- When a customer requests payment to be taken from a 3rd party;
- When a customer suddenly makes larger than expected payments.

The above list is not exhaustive.

25. Sanction monitoring

The UK sanctions regime Sanctions and Anti-Money Laundering Act 2018 came into effect 31st December 2020, this was a transition from EU regimes and allows the UK to establish their own UK

laws on sanctions. The Act applies to the whole of the UK.

The Government maintains a 'consolidated list' of individuals and entities that are based in the UK or elsewhere that are subject to financial sanctions. The Consolidated List is available at https://www.gov.uk/government/publications/the-uk-sanctions-list.

Sanction monitoring obligations under the UK financial sanctions regime apply to all firms; however, the Joint Money Laundering Steering Group expects measures put into place to be proportionate.

Firstsource has considered the complexity, processes, systems and operating environment and has classified the company in the UK to be of low risk. As a provider of business process outsourcing services, Firstsource always ensure sanction monitoring is completed for our Clients before entering into a relationship and then on an annual basis. We also ensure our Clients carry out regular sanction monitoring in respect of their customers and have robust policies and procedures in place to feedback information when it is relevant to Firstsource, in order that we may act upon it.

26. Court orders and warrants

Occasionally Firstsource may receive a request from The National Crime Agency (NCA) or another authority, who have obtained a production order through a Circuit Judge, or, in Northern Ireland, a County Court Judge, under the Police and Criminal Evidence Act (PACE). This Production Order allows the person named to obtain information of copy documents in order to investigate whether an individual has benefited from criminal conduct. These requests will, in the main, be directed to our clients and should be escalated as soon as possible under the Client process. Where Firstsource is the company named in the order the request should be sent immediately to Legal and Compliance at ukcompliance@firstsource.com.

When Legal and Compliance receives a request they must establish that the request is genuine and signed appropriately before fulfilling. We may occasionally receive requests from the Police, the Department of Works and Pensions or another official source; without a production order these must be refused and an official order requested.

There are several types of orders; the most relevant to Firstsource are listed below.

27. Interim receiving order

Where there is a risk of dissipation whilst investigations are being carried out, NCA may ask the High Court for an Interim Receiving Order, which freezes the identified property and gives the Interim Receiver addition investigative powers to determine whether the property in the Order is recoverable or is an associated property, arising from the same unlawful conduct.

28. Property freezing order

Property Freezing Orders enable the prosecuting authorities to apply for a free-standing order an as an alternative to an Interim Receiving Order, this is dependent on the nature of the case and the assets involved. This Order has the advantage of a speedier process, as an appointment of a Receiver is not required.

29. Restraint order

Legislation recognises that criminals under investigation, who may be eventually served with a Confiscation Order, may attempt to dispose of his property or attempt to put it out of the reach of the authorities. To prevent this from happening, authorities may serve Firstsource with a Restraint Order, specifying the restrictions which should operate against the account.

30. Confiscation order

Confiscation Orders can only be made by the Crown Court following conviction. The Courts can impose a penalty of up to £5,000 on Firstsource for not complying with this Order

If any of the above Orders are received they should be sent to the Financial Crime Team (FCT) immediately, in order for them to flag the account and ensure the instructions within the Order are recorded.

In order to ensure we do not contravene the terms of the Order, if any of the following are requested on an account which has been flagged as having received an Order, the account must be immediately referred to the FCT to gain express permission to continue with the request.

31. Politically Exposed Persons (PEP)

PEPs (as well as their families and persons known to be close associates) are required to be subject to enhanced scrutiny by firms subject to the Regulations. This is because international standards issued by the Financial Action Taskforce (FATF) recognise that a PEP may be in a position to abuse their public office for private gain.

See appendix 2 for ‘who is considered a PEP’.

It is the responsibility of the Money Laundering Reporting Officer of his deputy to conduct due diligence for all Clients and Suppliers.

32. Fraud

This policy aims to protect the brand, reputation and assets of the Company from loss or damage

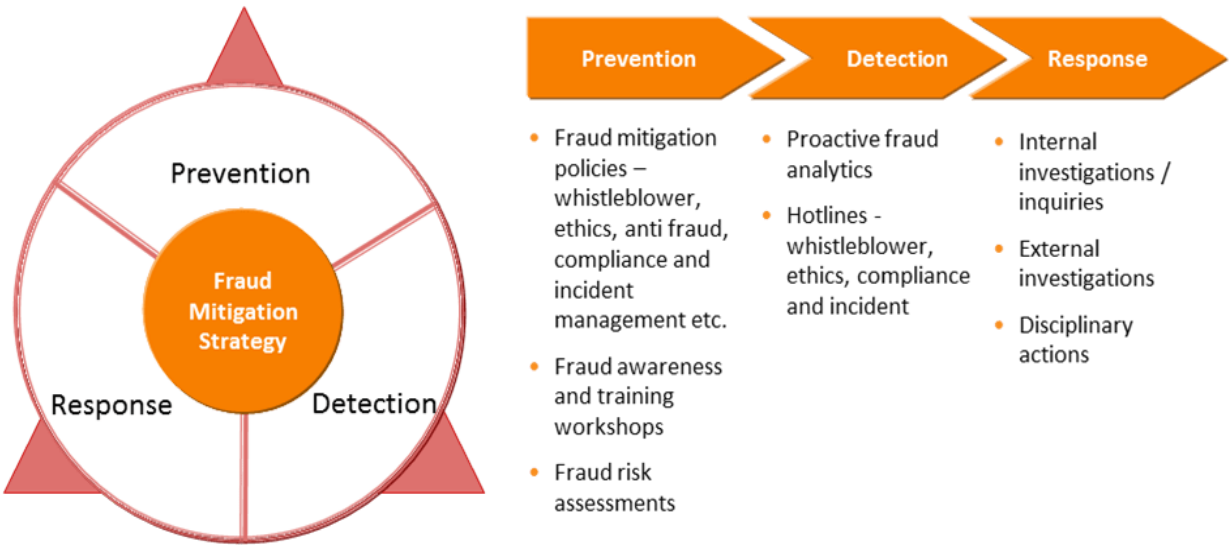
resulting from suspected incidents of fraud, in addition to safeguarding the confidentiality of client and customer data used for providing services to our clients.

- The policy has the following objectives:
- Promote zero tolerance to fraud;
- Strengthen the anti-fraud culture;
- Spread awareness and educate employees on fraud risks faced by the Company;
- Encourage all employees / associates of Firstsource to report cases of fraud; and
- Identify and address organization vulnerabilities through proactive and reactive measures

33. Fraud mitigation strategy

Firstsource's Fraud Mitigation Strategy focuses on fraud prevention, detection and response ("Three Pillars" of Fraud Risk Management) to achieve the following objectives:

- Proactive identification and remediation of fraud risk;
- Educate and guide employees and strengthen fraud preparedness; and
- Timely fraud response through investigations, disciplinary actions and process remediation.



34. Fraud prevention & control

Prevention of fraud is everybody's responsibility. Management, employees and associates of Firstsource] are expected to be alert at all times and take necessary steps to report fraud. Firstsource has a Fraud Management Team (FRM) in place globally with robust policies in place for Anti Bribery and Gifts and Entertainment to counter Bribery and Corruption threats; their responsibilities are listed below:

- Design and develop the FRM framework;
- Review, monitor, improve and implement security controls across the organization;
- Assess and approve adequacy and appropriateness of security / fraud controls across all organizational functions covering operations, administration, facilities, physical security, human resources, technology, finance, sales & marketing and other support functions;
- Assess, examine and approve inter as well as intra departmental controls;
- Sign off the policies, procedures and control designs for all departments covering the security / fraud prevention controls;
- Access systems, policies, records, documents, SOPs, MIS, employees (team members) and any other information of all functions / departments across the Company, with the approval of any member of the Risk Committee, as and when the need arises;
- Review and assess all reported cases of fraud;
- Manage / conduct / coordinate all investigations and share reports with the designated personnel;
- Recommend and follow through the disciplinary actions taken against the wrongdoers; and
- Review and update, as necessary, the Global Anti-Fraud Policy on an annual basis.

35. Inquiry & investigation

All reported incidents of suspected fraud will be reviewed and assessed and the required inquiries / investigations / inspections carried out. Firstsource may hire/involve the services of external / internal fraud investigation and / or forensic experts, wherever required. Further, all investigations will be handled on a case by case basis and may involve reporting to the Law Enforcements Authorities, where deemed necessary.

All investigations will be carried out objectively, and independently of the Line Management for the area in which the fraud has occurred or is suspected. All employees and third parties are required to provide complete support during all investigations.

Recommendations and disciplinary actions will be made on a case by case basis and learnings will be shared with relevant stakeholders to proactively manage and prevent similar cases in future.

36. Disciplinary actions

Disciplinary action will be taken against the perpetrator(s) in the event of an incident of fraud, which may involve but not limited to suspension or termination of employment, penalty, criminal or civil action. The disciplinary actions will be decided on a case by case basis.

37. Safeguarding

The confidentiality of all the information received will be maintained. Results of investigation conducted shall not be disclosed to anyone other than those who have a legitimate need to know.

Bad faith allegations: Notwithstanding anything contained anywhere in this policy, Firstsource shall have the absolute authority to take disciplinary action against the informant if it is found, upon investigation, that the allegations were made by informant in bad faith.

38. Awareness

Employee awareness with respect to fraud is critical and it is important that all employees understand the reporting modes and their responsibilities.

All employees in managerial positions will be responsible for educating their team members on the importance of complying with Global Anti-Fraud Policy and identifying / reporting of suspicious activity, at all times.

Additionally, fraud awareness training and refresher programs will be carried out on an annual basis. Managers and above will go through computer based training, declarations and assessments with a passing score of 90%.

Fraud can be classified into two broad categories, embezzling and identity theft. In the case of embezzling the cash is taken directly from the organisation and in the case of identity theft a

customer's personal information is misappropriated by the employee in order to make a profit.

At Firstsource, we foster an open communication culture. Any person (employee or associates of the Company) with knowledge of suspected incident of fraud or who is personally being coerced by others to participate in a fraudulent activity must report the case immediately.

All cases of suspected fraud can be reported to ukcompliance@firstsource.com or the Money Laundering Reporting Officer and the Company shall strive to maintain any request for anonymity.

Carefully refer to the important aspects to be considered while reporting a suspected fraud incident.

39. Information security controls

In order to aid the combating of fraud, Information Security has robust measures in place to ensure only staff with a genuine requirement have access to areas and computer systems appropriate to their role.

40. Gifts and entertainment

Firstsource has a robust Gifts and Entertainment policy in place, which can be found on the Intranet, this policy is designed to ensure compliance with Firstsource's ethical values and to:

- Comply with the UK Bribery Act 2010 ("UKBA") and the US Foreign Corrupt Practices Act 1977 ("FCPA") and other applicable anti-bribery and corruption laws; and
- Help Firstsource Personnel make the right decisions when providing or receiving gifts and entertainment while conducting business on behalf of Firstsource.

Firstsource have a zero tolerance for the provision and receiving of gifts or entertainment in breach of this Policy. Any breach of this Policy will be treated seriously by Firstsource and is likely to result in disciplinary action including without limitation, termination of employment.

This Gifts and Entertainment Policy ("Policy") applies to all Firstsource employees, officers, Board of Directors, consultants, vendors, trainees, interns, agents and representative (Firstsource Personnel).

41. Bribery and corruption

Firstsource values its reputation for conducting business in an ethical and transparent manner. It also recognises that it would suffer tangible and intangible losses including reputational losses, if there is

an involvement in bribery by the company and/or any of its employees, agents, representatives, vendors or business partners.

42. Reporting

The prevention, detection and reporting of bribery is the responsibility of all Firstsource Personnel and Third Parties. Firstsource is committed to ensuring that all Firstsource Personnel have a safe, reliable, and confidential way of reporting any suspicious activity.

Any concerns regarding bribery can be reported to the Money Laundering Reporting Officer or his deputy at ukcompliance@firstsource.com or at whistleblowing@firstsource.com. This reporting mechanism is available to Firstsource Personnel as well as Third Parties. The report should be made as soon as possible upon receiving a request for accepting or making a bribe, or upon belief that any of the terms of this Policy may have been violated.

43. Political contributions

Firstsource prohibits receiving or offering (directly or indirectly) remuneration, gifts, making any payments or donations or providing comparable benefits to any political party, political party officials or candidate on its behalf or using any of its resources or funds for any such purpose whatsoever.

44. Expense reimbursements

Only permitted expenses will be reimbursed in accordance with the Expenses Policy. Full details of any expenses will need to be provided along with details of individuals participating in the event and all relevant supporting documentation, such as, invoices or receipts. Employees submitting any inaccurate or misleading claims will be liable for disciplinary action, up to and including termination. For further details of expense reimbursement, the Expenses Policy can be found on the intranet.

45. Market abuse and personal account dealing

Firstsource has measures in place to ensure members of staff are not able to profit from access to information regarding companies or markets that have not been made public. All Directors are asked

to declare external interests and all members of staff must complete an annual declaration of interest, including share dealings.

46. Obligations

All members of staff must:

- Comply with this policy and the minimum standards relating to Financial Crime and Anti-Bribery and Corruption (this includes completing training and complying with relevant departmental processes, procedures and record retention guidelines).
- Must identify and verify all customers/entities/individuals (including directors and beneficial owners before entering into a relationship and throughout the lifecycle of the relationship as per policies and procedures provided by Firstsource and the Client.
- Report all cases of suspected fraud immediately on ukcompliance@firstsource.com or to the Money Laundering Reporting Officer.
- Escalate any suspicious external fraud activity as per Client guidelines and instructions.
- Comply with flagged restrictions on customer accounts as per Clients guidelines and instructions.
- Mitigate the risk of internal fraud by adhering to segregation of duties.
- Declare gifts and entertainment as and when they occur.
- Declare breaches of policy via the Breach Register.

Accountable Senior Management must ensure:

- All staff (full and part-time, permanent or temporary; contract staff; agents; consultants) within their area of responsibility have completed their annual Financial Crime Training and they can supply documented evidence.
- All staff complete Client Financial Crime training and are fully aware of the policies and procedures applicable to their role.

Firstsource is required by the FCA to ensure that all staff in financial services firms are accountable for their decisions. In light of this all staff are required to complete mandatory training in relation to the Senior Manager's and Certification Regime.

Furthermore, authorised or senior members of staff will be required to undertake a 'fit and proper test' annually.

Client Directors will ensure:

- Financial Crime is discussed at Client meetings.
- Financial Crime is always considered when assessing risks for their areas.
- Information Security is alerted to changes of personnel to ensure access to systems and areas are immediately restricted.
- Regularly communicate the Company's message of honesty and integrity with employees of the Company, through the Employee Handbook and other written and verbal presentations of the principles underlying in this Policy.
- Conduct periodic meetings to ensure employees attend trainings regarding business ethics and the related laws and regulations.

All Recruiting Managers will ensure they:

- Comply with the employee vetting policy and ensure new personnel have been subject to vetting and Criminal Record Board checks prior to commencing employment.
- Obtain Declaration for reading, understanding and agreeing to comply with the Global Anti-Fraud Policy from all employees.

The MLRO and/or his deputy will:

- Act as an internal control point for procedures, legislation, inspection, reporting, co-ordination, training and internal communications.
- Produce an annual 'MLRO report' that covers key Financial Crime issues.
- Review this Financial Crime policy and procedure document where and when important changes have occurred or annually as a minimum; and, escalate new version to all stakeholders.
- Review Financial Crime training where and when important changes have occurred or annually as a minimum; and, escalate new version to all stakeholders.
- Maintain an open and transparent relationship with the regulators, law enforcement and other bodies in relation to financial crime prevention.
- Conduct Due Diligence for each supplier and client. Where due diligence is being conducted by a third party, formal instructions must be provided and evidence obtained for record keeping purposes. These records will be retained for a minimum of 5 years after the business relationship ends.

- Carry out Sanction Monitoring before entering into a relationship and then annually.
- Will ensure where a weakness has been identified, remediation will be monitored to ensure remediation.
- A Gift and Hospitality policy and procedure is in place and reviewed annually or when significant changes have been made.
- Conduct appropriate investigation of suspected financial crime and take appropriate action where necessary.
- Recommend and follow through the disciplinary actions taken against wrongdoers.

47. Appendix 1 - Suspicious activity report

REPORTER DETAILS		
Name	**Department/Client Contract**	**Contact Details**

Reason for Suspicion
(Full details should be given here, including details of investigations carried out, reference points etc)
Have you attached evidence **Yes** **No**

Name	**Signature**	**Date**

48. Appendix 2 – who should be treated as a PEP?

PEPs are defined as individuals entrusted with prominent public functions, including:

- Heads of state, heads of government, ministers and deputy or assistant ministers.
- Members of parliament or of similar legislative bodies – similar legislative bodies include regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers. It does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.
- Members of the governing bodies of political parties – the FCA considers that this only applies to political parties who have some representation in a national or supranational Parliament or similar legislative body as defined above. The extent of who should be considered a member of a governing body of a political party will vary according to the constitution of the parties, but will generally only apply to the national governing bodies where a member has significant executive power (e.g. over the selection of candidates or distribution of significant party funds).
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances – in the UK this means only judges of the Supreme Court; firms should not treat any other member of the judiciary as a PEP and only apply EDD measures where they have assessed additional risks.
- Members of courts of auditors or of the boards of central banks.
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces – the FCA considers this is only necessary where those holding these offices on behalf of the UK government are at Permanent Secretary/Deputy Permanent Secretary level, or hold the equivalent military rank (e.g. Vice Admiral, Lieutenant General, Air Marshal or senior).
- Members of the administrative, management or supervisory bodies of State owned enterprises – the FCA considers that this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises.
- Directors, deputy directors and members of the board or equivalent function of an international organisation – the FCA considers that international organisations only includes international public organisations such as the UN and NATO.

*** taken from FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes