

Financial Crime Policy

Master List Ref COM001	Release Date August 2015	Review Date January 2026	Next Review Date January 2027
Version: 5.3	Process Owner Legal & Compliance	Reviewed by MLRO	Approved by UK Board

This document is the sole property of Firstsource Solutions UK Limited ("FSUKL"). Any use or duplication of this document without the express permission of FSUKL is strictly forbidden and illegal.

Contents

1.	Definitions	3
2.	Scope.....	4
3.	Applicable law and regulation.....	5
3.1	Money Laundering and Terrorist Financing	5
3.2	Bribery Act 2010 (BA 2010).....	6
3.3	Failure to Prevent Fraud Offence (FTPF).....	6
3.4	Sanctions.....	7
4.	Risks.....	7
5.	Third Parties.....	7
5.1	Applicability of the policy to third parties.....	Error! Bookmark not defined.
5.2	Third party acceptance policy.....	7
6.	Board statement.....	8
7.	Training	8
7.1	Timing and approach to training	9
8.	Money laundering.....	9
8.1	What is Money Laundering	9
8.1.1	Placement.....	9
8.1.2	Layering.....	9
8.1.3	Integration.....	9
8.2	Financing or facilitating terrorism	10
8.3	How to identify money laundering	11
8.4	What to do if you suspect money laundering?.....	11
8.5	Reporting obligations under POCA 2002.....	11
8.6	Notifications and consent under POCA 2002 from the NCA	12
8.7	Money laundering offences and penalties under POCA 2002.....	13
8.7.1	Section 327.....	13
8.7.2	Section 328.....	13
8.7.3	Section 329.....	13
8.8	Offences applicable to FSUKL.....	13
8.9	Offences applicable to Clients	14
9.	Sanction monitoring.....	14
10.	Court orders and warrants	15
10.1	Interim receiving order	15
10.2	Property freezing order	15
10.3	Restraint order.....	16
10.4	Confiscation order.....	16

11.	Fraud	16
11.1	Failure to Prevent Fraud offence (FTPF).....	16
11.1.1	Top level commitment.....	17
11.1.2	Risk assessments	17
11.1.3	Proportionate risk-based fraud prevention procedures.....	17
11.1.4	Due diligence.....	17
11.1.5	Communication.....	17
11.1.6	Monitoring and review.....	18
11.2	Fraud mitigation strategy.....	18
11.3	Fraud prevention & control.....	18
12.	Bribery and corruption.....	19
13.	Associated Persons	19
13.1	Employees responsibilities.....	19
13.2	Relevant Associated Persons.....	20
13.3	Appointing Third Parties	20
14.	Gifts and Hospitality.....	20
15.	Other activities requiring close attention.....	21
15.1	Facilitation Payments.....	21
15.2	Political Contributions	21
15.3	Charitable Contributions.....	21
16.	Market abuse and personal account dealing.....	22
17.	Appendix 1 - Suspicious Activity Report.....	23
18.	Version Control.....	24

1. Definitions

Term	Definition
AML	Anti-money laundering
AML Compliance Program	FSUKL anti-money laundering compliance program
Associated Person	Means employees, agents, subsidiaries and other persons who provide services for or on behalf of FSUKL
BA 2010	Bribery Act 2010
Board	FSUKL Board of Directors
Breach Register	[FSUKL Breach Register]
Client	An entity which FSUKL provides services to as part of its business outsourcing provider model
Customer	A customer of a Client
ECCTA 2023	The Economic Crime and Corporate Transparency Act 2023
Employee Handbook	Firstsource Employee Handbook
FATF Blacklist	Financial Action Taskforce Blacklist
FCA	Financial Conduct Authority
FCA Handbook	Financial Conduct Authority Handbook; rules and guidance issued by the Financial Conduct Authority
FCT	Financial Crime Team
Financial Crime	Any kind of criminal conduct relating to money or to financial services or markets, including any offence involving: • Fraud or dishonesty; • Misconduct in, or misuse of information relating, a financial market; or • Handling the proceeds of crime; or • The financing of terrorism.
Financial Sanctions List	FATF's High Risk Third Countries where there is an assessed high risk of money laundering or terrorist financing
Firstsource or Group	Firstsource Solutions Limited and its subsidiaries and affiliates.
FRM	Fraud Management Team
FSUKL	Firstsource Solutions UK Limited
FTPF	The Failure to Prevent Fraud
Global Anti-Bribery and Gift & Entertainment Policy	Firstsource Global Anti-Bribery and Gift & Entertainment Policy
Global Anti-Fraud Policy	Firstsource Global Anti-Fraud Policy
JMLSG	Joint Money Laundering Steering Committee Guidance
MI	Management Information
MLRO	Money Laundering Reporting Officer
MLRs 2017	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017/692
NCA	National Crime Agency
Nominated Officer	At present, the MLRO has assumed Nominated Officer responsibilities however at a point in the future a separate Nominated Officer may be appointed
OFAC	Office of Foreign Assets Control
PACE	Police and Criminal Evidence Act
POCA 2002	The Proceeds of Crime Act 2002
Policy or Policies and Procedures	This Financial Crime Policy
Risk Committee	FSUKL Risk Committee
SAMLA 2018	Sanctions and Anti-Money Laundering Act 2018
SAR	Suspicious Activity Report
Senior Manager/Director(s)	FSUKL Senior Manager/Director(s)

2. Scope

This policy is relevant to all employees and third party suppliers. Employees includes the directors, permanent and fixed-term employees, consultants, contractors, trainees, interns, part-time, full-time, casual workers and temporary agency workers, agents, and appointed representatives acting on behalf of FSUKL.

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

The purpose of this Policy is to protect the brand, reputation and assets of FSUKL 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 FSUKL.
- Encourage all employees / associates of FSUKL to report suspicions of Financial Crime.
- Identify and address organisation vulnerabilities through proactive and reactive measures.

This document sets out the policy for FSUKL and is a minimum requirement.

Where FSUKL is contracted to work on behalf of a client and is required to follow client procedures, FSUKL will complete an exercise prior to commencing the contract to compare the relevant FSUKL policies against the client policies and procedures to ensure that as a minimum FSUKL policies are being met. Where there are gaps, these will be discussed with the client. The same exercise and approach will be adopted as part of any mid-contract change control process.

To ensure clarity of responsibility and to avoid duplication or inconsistency:

- Where an activity is performed solely on behalf of a client, and the client has established policies and procedures governing that activity, FSUKL will follow those policies and procedures, provided they are consistent with applicable UK laws, regulatory expectations and FSUKL's own standards.
- This policy applies in all situations where FSUKL has its own legal or regulatory responsibilities, and where the matter concerns FSUKL's own internal operations, staff, processes, systems or data.
- This policy applies where FSUKL identifies a material gap, failure, or inappropriate action within a client's control environment, or where we reasonably believe that client-owned processes may not ensure compliance with applicable UK law or regulatory requirements.

3. Applicable law and regulation

FSUKL is an entity which is authorised and regulated by the Financial Conduct Authority (**FCA**). As a result of being a regulated entity, it is subject to the provisions of the FCA Handbook and is required to make sure it has adequate systems and controls in place in order to comply with its obligations under this sourcebook.

As an entity which has to comply with this sourcebook it is essential to consider all systems and controls to ensure that it can minimise risk and harm arising from Financial Crime. Financial Crime is defined broadly and is “any kind of criminal conduct relating to money or to financial services or markets, including any offence involving:

- Fraud or dishonesty;
- Misconduct in, or misuse of information relating to, a financial market; or
- Handling the proceeds of crime; or
- The financing of terrorism.

To ensure that the controls are adequate, FSUKL is required to consider a broad range of legislation including:

- The Bribery Act 2010 (**BA 2010**)
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017/692 (**MLRs 2017**);
- The Proceeds of Crime Act 2002 (**POCA 2002**); and
- The Economic Crime and Corporate Transparency Act 2023 (**ECCTA 2023**); and
- Sanctions and Anti-Money Laundering Act 2018 (**SAMLA 2018**).

3.1 Money Laundering and Terrorist Financing

The primary legislation that applies in respect of anti-money laundering and terrorist financing is the MLRs 2017. The MLRs 2017 only apply to certain types of entity. FSUKL does not fall within scope of the MLRs 2017 due to its business activities. However, a large number of its Clients fall within scope of the MLRs 2017. Therefore, FSUKL is contractually obliged to implement certain client arrangements and processes to ensure that it acts in a manner which is compliant with the MLRs.

This Policy sets out the systems and controls which FSUKL has implemented in order to prevent money laundering and terrorist financing in accordance with its contractual obligations. Additionally, whilst the requirements of the MLRs 2017 do not apply directly to FSUKL, certain obligations on regulated entities which apply to the Clients of FSUKL are highlighted in this Policy.

Where an individual has a suspicion of money laundering, they are required to report such suspicion internally and to the relevant nominated officer (Client or FSUKL and dependent on the nature of the suspicion). Where the nominated officer agrees with the suspicion of money laundering, the requirement is that the nominated officer makes a report to the National Crime Agency (**NCA**).

The Joint Money Laundering Steering Committee Guidance (**JMLSG**) aims to provide guidance to firms on implementing the requirements of the FCA and the MLRs 2017. As a number of its Clients comply with the requirements of JMLSG, FSUKL notes the requirements as best practice and has built the requirements of the JMLSG into its processes.

As an FCA regulated entity, FSUKL needs to consider the requirements of the [FCA's Financial Crime Guide](#) and best practice outlined therein.

Further guidance on Money Laundering and Terrorist Financing is provided in [Section 8](#).

3.2 Bribery Act 2010 (BA 2010)

The BA 2010 sets out the corporate offence of failure to prevent bribery. Very broadly, all UK incorporated commercial organisations and those commercial organisations which are conducting business in the UK are subject to the requirements of the BA 2010 and therefore obliged to implement controls to prevent bribery.

The Ministry of Justice has published [guidance](#) for commercial organisations which sets out six principles for businesses to comply with to evidence that they have implemented appropriate systems and controls to prevent bribery.

In a commercial context (that is not involving foreign public officials) for there to be an offence under the BA 2010, the prosecution must show that the hospitality in question:

- Provided a financial or other advantage to another person; and
- Was offered or given with the intention of inducing the person to perform a relevant function improperly or in the knowledge of acceptance of the advantage would in itself be improper performance.

It should be understood that improper performance of a function is a performance that amounts to a breach of an expectation that a person will act in good faith, impartially or in accordance with a position of trust.

It is also an offence to bribe a foreign public official. This offence occurs where there is a bribe that is intended to influence the foreign public official in their capacity as a foreign public official.

Separately, FSUKL commits an offence if a person bribes another person (including a foreign public official), and the bribe is with the intention of obtaining or retaining business for FSUKL or obtaining or retaining an advantage in the conduct of business for FSUKL.

The BA 2010 covers offences committed inside the UK and outside the UK where the person committing them has a close connection with the UK by virtue of being a British national or ordinarily resident in the UK. Additionally, failure of a commercial organisation to prevent bribery applies to any entity which carries on business, or a part of a business in the UK (such as FSUKL).

Differing laws in other countries and regions where activities take place, differing cultural differences, local practice and business custom will only be considered if it is formally enshrined in that jurisdiction's law.

Further guidance is provided in [Section 12](#).

3.3 Failure to Prevent Fraud Offence (FTPF)

The ECCTA 2023 has introduced a new offence, FTPF. The offence makes an organisation liable if it fails to prevent a specified fraud offence (see details below) from being committed where: (i) an employee or agent commits the fraud; and (ii) the fraud is intended to benefit the organisation or a person to whom services are provided on behalf of the organisation.

Only certain types of fraud are captured by FTPF, but a number of them will be relevant to FSUKL as a large UK corporation including fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.

Importantly, the offence has a defence of “reasonable procedures” to prevent fraud. This means FSUKL is required to implement anti-fraud systems and controls to cover fraud committed for their benefit by employees, subsidiaries or third-party agents.

The territorial scope of the offence is broad and will capture activities of a UK incorporated entity such as FSUKL where the fraud occurs in the UK. Further guidance is provided in [Section 11](#).

3.4 Sanctions

Sanctions are an important part of the prevention of Financial Crime, and dependent upon the specific jurisdiction and where an entity conducts its activity will dictate which sanctions with which it needs to comply. The SAML 2018 creates the power for the UK government to implement a broad range of sanctions and comply with its UN obligations.

Organisations are required to comply with sanctions which are implemented by the UK government and therefore it is essential that FSUKL implements policies and procedures to regularly check sanctions lists and consider whether any third parties or Clients are subject to sanctions. Further guidance is provided in [Section 9](#).

4. Risks

This Policy reduces the following risks:

- FSUKL or its Clients 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 FSUKL due to inadequate processes and controls.

5. Third Parties

5.1 Third Party Acceptance Policy

Prior to FSUKL initiating contracts with any third parties, clients or suppliers, a background verification check must be 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 FSUKL regulatory obligations and to deliver our services in an ethical and transparent manner. These checks include:

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

The list is not exhaustive – if you are unsure or have any queries on third parties or suppliers, please contact the Legal and Compliance team at ukcompliance@firstsource.com and they will be happy to answer any queries you may have.

6. Board statement

FSUKL is required 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 UK 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 Anti-Money Laundering (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 anti-money laundering (**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 POCA 2002 states that the absence of adequate training by an employer, as required by the regulations, will provide a defence for staff against a criminal charge of not reporting knowledge or suspicion of money laundering. The defence 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 FSUKL 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.

7.1 Timing and approach to training

Training is provided in three ways:

- Training on induction by both the Client (where applicable) and FSUKL;
- Annual training by both Client (where applicable) and FSUKL;
- 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 regular 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.

8. Money laundering

8.1 What is 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 laundering has three primary stages, which collectively encompass the necessary steps to turn "dirty" money into "clean" money and make the funds appear to be legitimately sourced. The three stages are summarised below:

8.1.1 Placement

This involves placing the 'dirty' money into the legitimate financial system. This stage can occur in a number of ways including placing funds into off-shore bank accounts, putting a large number of small amounts across several bank accounts or alternatively invoicing an entity in a fraudulent way. From the perspective of FSUKL and its Clients, it may identify this stage when Clients suddenly make large cash overpayments on loans or mortgages or ask to use several bank accounts to make payments.

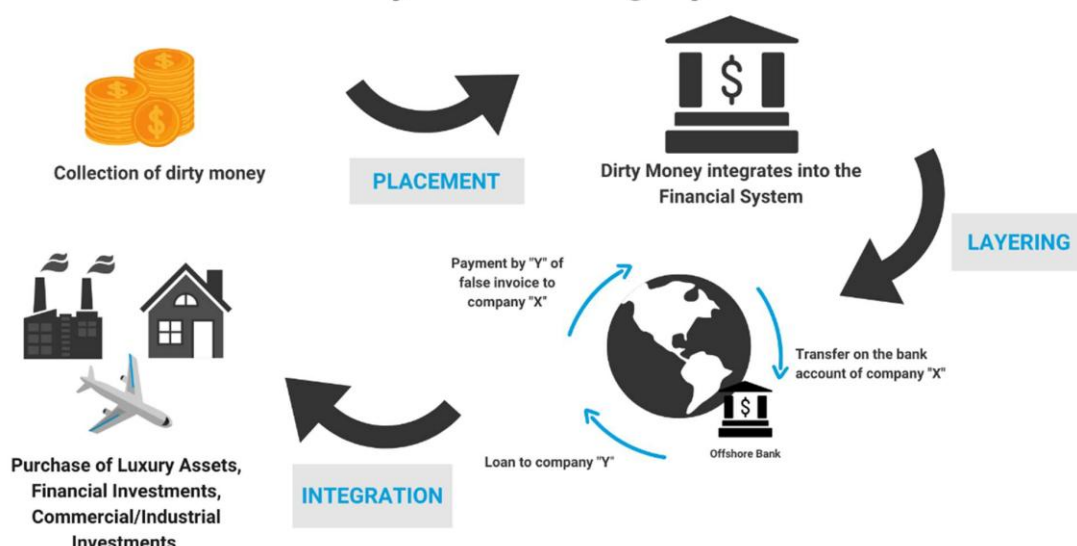
8.1.2 Layering

This stage is a series of sophisticated financial transactions, usually involving offshore techniques to limit the audit trail regarding the illicit source. The ultimate goal is to generate so many financial transactions that the original source of the funds is obscured.

8.1.3 Integration

At this point the laundered money has been absorbed into the legal financial system and is legal tender for criminals to use. Real estate transactions are often used for the purposes of integration. A diagram of how the three stages work are set out below.

Money Laundering Cycle



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 MLRs 2017.

The POCA 2002 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.

8.2 Financing or facilitating terrorism

It is a criminal offence to finance or facilitate the financing of terrorism, and there are legal obligations under POCA 2002 to submit Suspicious Activity Reports (SAR) when we suspect criminal activity. We supply training and guidance to all staff to ensure they are aware of the laws designed to prevent money laundering and terrorist financing.

FSUKL 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.

A copy of the FSUKL SAR report is available in Appendix 1.

8.3 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 Sanctioned individuals or jurisdictions (see [Section 9](#)).
- Is there evidence of unsupported customer wealth, both in individual and corporate clients? This should trigger further questions.

8.4 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 the relevant Client or FSUKL function – for FSUKL, this is ukcompliance@firstsource.com. A copy of the SAR can be found in Appendix 1. The Legal and Compliance team will create a SAR register as and when required to review any reported activities and to mitigate any risks or patterns should they occur.

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 regulated sector. A number of Clients, including Oodle and LBG are part of the regulated sector and therefore are subject to their own reporting obligations.

8.5 Reporting obligations under POCA 2002

The reporting obligations in POCA 2002 are applicable to anyone in the UK that may interact with an individual or business, whereby they may commit a money laundering offence. Due to the permissions it holds, FSUKL is not considered as being in the “regulated sector”. However, due to FSUKL’s client base, FSUKL upholds high standards and expects any individual who has concerns or questions regarding money laundering or suspects money laundering to report this to the nominated officer. The nominated officer can be reached through the Legal and Compliance team on ukcompliance@firstsource.com. In the event that the nominated officer does not make a report when there is a reasonable suspicion of money laundering, then the nominated officer may be guilty of an offence.

Certain Clients who are part of the “regulated sector” have their own reporting obligations and have set out specific procedures which FSUKL needs to follow. It is very important you follow those procedures in the event of supporting one of those Clients and follow the reporting procedure mandated for that Client. That may include making a SAR report. A copy of the internal SAR report which should be used to make a report to the nominated officer can be found at Appendix 1.

FSUKL regularly communicates to all employees the importance of reporting any suspicions as soon as any employee suspects any such activity has been committed as part of its compliance framework.

<u>Important: Do's</u>	<u>Important Don'ts</u>
• 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 evidence 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.	• Do not delay in reporting the incident. The more you delay, the longer the exposure for FSUKL • 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. • Do not alert the person suspected of the criminal activity as this is called 'tipping off' and doing so can be an offence

8.6 Notifications and consent under POCA 2002 from the NCA

There are two possible types of reports which can be made to the NCA:

- Notifications; and
- "Consent" applications

Notifications are made where there is a suspicion of money laundering, but FSUKL does not hold any money or property of the person which it has suspicions of committing money laundering. This means making an appropriate notification to the NCA regarding the nature of the suspicion so that it can then take any steps it considers necessary and appropriate to investigate the suspicion.

Consent applications are applications made to the NCA to allow the entity to take some action with potential criminal property (which includes funds) where there is some suspicion of a person committing a money laundering offence. This is acting in respect of such criminal property may constitute an offence under POCA 2002.

The Client or FSUKL Nominated Officer is responsible for making a report under POCA 2002 to the NCA. No other individual from FSUKL should make a direct report to the NCA.

The 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 Nominated Officer / 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.

All staff are required to notify the nominated officer about a suspicion of money laundering using the SAR form at Appendix 1. If a SAR is made to the NCA, the relevant Nominated Officer will instruct you as to how to proceed with any Customer or Client relationship.

8.7 Money laundering offences and penalties under POCA 2002

The three principal money laundering offences are contained in sections 327, 328 and 329 of POCA 2002. These offences are punishable by a maximum of 14 years' imprisonment and/or a fine. The MLRO 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 NCA.

For Clients, additional offences exist and in particular there are obligations on their Nominated Officer to file reports.

8.7.1 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.

8.7.2 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.

8.7.3 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.

8.8 Offences applicable to FSUKL

Offence

Prejudicing an investigation into Money Laundering investigation by making a disclosure or falsifying, concealing or destroying other documents which are relevant to the investigation.

Penalty

Up to 5 years imprisonment and/or fine.

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

Up to 14 years' imprisonment and/or fine.

8.9 Offences applicable to Clients

Offence

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

Penalty

Up to 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

Up to 5 years' imprisonment and/or fine.

Offence

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

Penalty

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

Offence

The nominated officer fails to report if they acquire knowledge, or suspicion, of Money Laundering.

Penalty

Up to 5 years' imprisonment and/or fine.

9. Sanction monitoring

The UK sanctions regime SAMLA 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 SAMLA 2018 applies to the whole of the UK.

The Government maintains a 'consolidated list' of individuals, entities and jurisdictions that are subject to financial sanctions. FSUKL will not deal with any jurisdictions, individuals or entities that are sanctioned by the either UK, US or EU sanction restrictions. The following Sanctions list can be used as reference points for all current sanctions lists.

- [FATF Blacklist](#)
- [UK Sanctions List](#)
- [US Sanctions list](#)
- [EU Sanction List](#)

In the event a member of staff identifies a transaction related to an individual/entity/jurisdiction on any of the Sanctions lists it must be reported immediately to FSUKLs MRLO and to the Client, through the procedure you have been given.

Sanction monitoring obligations under the UK financial sanctions regime apply to all FSUKL clients; however, the JMLSG expects measures put into place to be proportionate.

FSUKL has considered the complexity, processes, systems and operating environment and has classified FSUKL in the UK to be of low risk. As a provider of business process outsourcing services, FSUKL 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 FSUKL.

10. Court orders and warrants

Occasionally FSUKL may receive a request from the 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 or 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 FSUKL is the company named in the order the request should be sent immediately to Legal and Compliance at ukcompliance@firstsource.com. Although it is unlikely, in the rare instances that a request is directed to FSUKL the reverse process will apply and it may be necessary to request information from a Client. If this occurs raise it with Legal and Compliance at the email address above.

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.

FSUKL very rarely holds client data on our systems and so it is unlikely a protection order will be made against FSUKL. However, in the event this does occur it should be sent immediately to Legal and Compliance at ukcompliance@firstsource.com.

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

10.1 Interim receiving order

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

10.2 Property freezing order

Property Freezing Orders enable the prosecuting authorities to apply for a free-standing order 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.

10.3 Restraint order

Legislation recognises that criminals under investigation, who may eventually be 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 FSUKL with a Restraint Order, specifying the restrictions which should operate against the account.

10.4 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 FSUKL for not complying with this Order

If any of the above Orders are received they should be sent to the Legal and Compliance at ukcompliance@firstsource.com, 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.

11. Fraud

This Policy aims to protect the brand, reputation and assets of FSUKL from loss or damage resulting from suspected incidents of fraud, in addition to safeguarding the confidentiality of Client and Customer data. This applies both to fraud committed against FSUKL, and fraud committed by employees or other persons associated with FSUKL against third parties.

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 FSUKL;
- Encourage all employees / associates of FSUKL to report cases of fraud;
- Identify and address organisation vulnerabilities through proactive and reactive measures; and
- Prevent FSUKL from committing the FTFP offence under the ECCTA 2023 (See [Section 11.1](#));

This Policy should be read in conjunction with Firstsource's Global Anti-Fraud Policy.

The Global Anti-Fraud Policy defines fraud as *"a wilful act committed by an individual or entity, by deception, suppression, cheating or by any other fraudulent or illegal means, thereby causing wrongful gain(s) to self and other individuals and wrongful loss to others"*.

11.1 Failure to Prevent Fraud offence (FTPF)

FSUKL may be the victim of fraud, such as one that is intended to benefit an employee or service provider through the payment of false expense claims or invoices. FSUKL also may benefit from fraud, such as where payments are received based on misrepresented information or a penalty is avoided because information was concealed.

The ECCTA 2023 introduces FTFP offence which makes an organisation liable if it fails to prevent a specified fraud offence from being committed where an Associated Person of the organisation commits the fraud; and the fraud is intended to benefit either the organisation itself or a person to whom services are provided on behalf of the organisation.

The definition of Associated Person has a broad scope and includes employees, agents, subsidiaries and other persons who provide services for, or on behalf of the relevant organisation. The key concept of the offence is that it is designed to prevent outward fraud, where the organisation benefits from the fraud, as opposed to inward fraud where the organisation is a victim of fraud.

The offence has a defence of “reasonable procedures” to prevent fraud, which requires organisations to conduct a risk assessment to identify areas in which fraud could be committed for the organisation’s benefit by their associated persons and to enhance their anti-fraud systems and controls to cover these frauds.

FSUKL is committed to following guidance published in the UK by the Home Office and UK Finance as set out below:

11.1.1 Top level commitment

- Responsibility for prevention and detection of fraud rests with the person filling the SMF16 function.
- The Board and FSUKL’s senior management takes a zero-tolerance approach towards fraudulent, dishonest and corrupt practices

11.1.2 Risk assessments

- FSUKL will carry out a risk assessment in relation to the FTFP offence, which will involve the identification of situations in which fraud could be committed by FSUKL or its Associated Persons and then assessing whether FSUKL’s controls are adequate to manage the risk of these frauds occurring.
- FSUKL commits to carrying out regular reviews of its risk assessment, in particular where there have been changes in the business or increases in risk.

11.1.3 Proportionate risk-based fraud prevention procedures

- FSUKL will put in place reasonable and proportionate fraud prevention procedures to manage the risks of fraud being committed by FSUKL or its Associated Persons.
- In doing so, FSUKL will consider the level of control and supervision that FSUKL is able to exercise over the associated persons.

11.1.4 Due diligence

- FSUKL will put in place proportionate and risk based due diligence procedures in respect of Associated Persons to mitigate identified fraud risks.

11.1.5 Communication

- FSUKL will ensure that its fraud prevention policies and procedures are communicated and understood throughout the organisation.
- FSUKL will also ensure that there is awareness and understanding of its policies from those that provide services on its behalf.

- FSUKL will incorporate training into its existing financial crime prevention training and consider whether enhanced training is required where there are greater perceived risks of fraud.

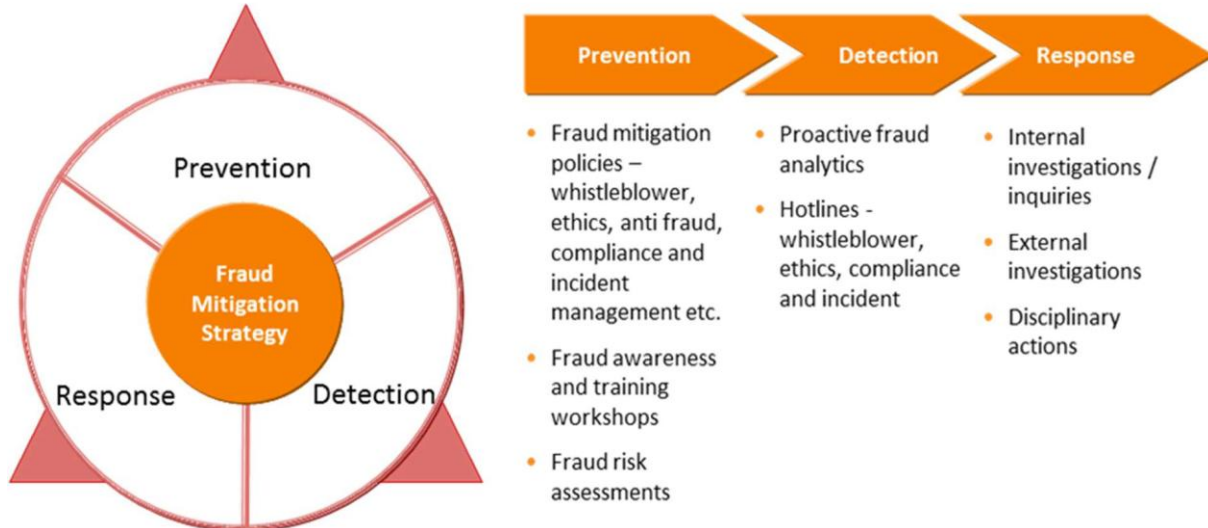
11.1.6 Monitoring and review

- On an ongoing basis, FSUKL will monitor and review its fraud detection and prevention procedures and make improvements where necessary. This will include:
 - Detection of actual and attempted fraud;
 - Investigations; and
 - Monitoring the effectiveness of fraud prevention measures.
- As the nature of risks faced by FSUKL may change over time, its fraud detection and prevention procedures will also have to adapt to take account of these risks.

11.2 Fraud mitigation strategy

FSUKL'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.



11.3 Fraud prevention & control

Prevention of fraud is everybody's responsibility. Management, employees and associates of FSUKL are expected to be alert at all times and take necessary steps to report fraud. FSUKL 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 organisation;

- Assess and approve adequacy and appropriateness of security / fraud controls across all organisational 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, procedures, Management Information Systems, employees (team members) and any other information of all functions / departments across FSUKL, 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.

12. Bribery and corruption

FSUKL 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 FSUKL and/or any of its employees, agents, representatives, vendors or business partners. This section should be read in conjunction with the Global Anti-Bribery and Gifts & Entertainment Policy.

13. Associated Persons

FSUKL could be held responsible for the actions of an Associated Person acting on its behalf. Care must be taken to ensure that those Associated Persons do not attempt to engage in any form of financial crime.

13.1 Employees responsibilities

When dealing with Associated Persons, employee must follow the following guidance:

- Ensure due diligence is conducted on any new Associated Persons (or those whose contracts are being renewed) who provide services on behalf of FSUKL.
- Payment to Associated Persons should be on commercially reasonable terms. Any payments to Associated Persons must be as provided under their contract which should also set out the detail of the services which they shall provide. Requests for one-off changes to the payments should be rejected unless the reason is clearly documented in writing.
- Undertake sufficient due diligence in relation to any proposed acquisition or joint venture to minimise the risk of financial crime.

13.2 Relevant Associated Persons

FSUKL has identified the following as types of Associated Persons it has relationships with:

- Full or part time employed members of FSUKL staff
- Full or part time employed members of FSL staff
- Appointed Representatives
- Clients
- Third-Party partners (for example, consultancy firms, and lawyers)
- Contractors
- External auditors

Contact the MLRO if you are unsure if a particular entity will qualify as an Associated Person.

13.3 Appointing Third Parties

FSUKL's zero-tolerance approach to financial crime should be communicated to all suppliers, contractors and business partners at the outset of a business relationship with them and as appropriate thereafter.

When contacting third parties to ask if they are free to act on behalf of FSUKL, early on, ask them to undertake a conflict check before giving them any sensitive information and ask them if they have in place systems and controls to mitigate bribery and corruption risk. It is important to note that when FSUKL issues instruction to third parties, it must be in writing and confirm that the third party:

- is aware of the instruction;
- understands the reason for the instruction;
- agrees to comply with UK standards of regulation pertaining to market abuse and insider dealing. Even if there is no explicit rule in the relevant region, it is essential for reputational reasons that UK standards are applied;
- agree to abide by the principles set out in this Policy; and
- Where there are concerns that the third party may not be familiar, and/or may not comply, with the UK anti-bribery and anti-corruption requirements, a request should be made to review the third party's own anti-bribery and anti-corruption controls. If concerns remain, it may be advisable for FSUKL to provide the third party with training.

14. Gifts and Hospitality

There are legitimate reasons for the occasional giving/receiving of gifts and business-related hospitality but this area can pose a risk where excessive gifts or hospitality could be viewed as a bribe and/or a conflict of interest. FSUKL follows the Global Anti-Bribery and Gifts & Entertainment policy.

The principles set out in the Group policy apply regardless of whether the gift or hospitality is to be provided to FSUKL's employee, a third-party employee or to members of their respective families, friends or acquaintances.

It is not the intention that genuine hospitality or reasonable and proportionate business expenditure should infringe the legislation. You can continue to provide/receive bona fide hospitality, promotion and other business expenditure. The intention of the legislation is to catch hospitality that is really a cover for corruption or bribery. In order to bring a case relating to provision of hospitality or promotional expenses, the prosecution would have to show that the hospitality was intended to bring about improper performance and this is judged by what a reasonable person in the UK would think. Local custom and practice is not a defence.

15. Other activities requiring close attention

15.1 Facilitation Payments

Facilitation payments are small unofficial payments to ensure or speed up performance of routine or necessary action. These will be seen as bribes under the BA 2010, regardless of whether they may be a part of the "way of doing business" in a particular country. As a representative of FSUKL, you must not make any facilitation payment.

15.2 Political Contributions

FSUKL is not a political organisation. It does not support political parties nor contribute funds to groups whose activities are calculated to promote party interests or the election of a specific candidate. In some limited instances, FSUKL may contribute funds towards organisations or entities that engage in the political process to address an issue that directly affects FSUKL and its business activity if:

- permitted by local law and regulation;
- supported by an appropriate level of due diligence;
- specifically approved by the UK Board.

15.3 Charitable Contributions

- Charitable contributions may only be given to recognised non-profit charitable organisations. It is important to ensure that FSUKL is only giving to legitimate charities that are not involved in Financial Crime or other corruption. All donations must be:
 - Transparent and properly recorded with the Compliance and Finance departments.
 - Receipted or have a letter of acknowledgement from the charity to ensure that the donations receive the proper tax treatment.
 - Have appropriate due diligence conducted to assess whether the charity:
 - is authentic;
 - has any connections, associations or links to political causes;
 - operates in, or send funds to, high-risk jurisdictions;
 - has been the subject of adverse media reports indicating financial crime or other irregularities.
- Donations must not:

- Be made to individuals or in cash; and
- Be made at the request of a public official as an inducement to or reward for acting improperly.

16. Market abuse and personal account dealing

FSUKL 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 where a members of staff has a conflict of interest, they must complete an annual declaration of interest, and any associated share dealings.

17. 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

18. Version Control

#	Date	Author	Summary of key changes	Approvers
5.2	14/01/26	Norton Rose	Legal input and refresh of existing financial crime policy	
5.3	16/01/26	Nick Allen	Additions and refinements answering questions from V5.2. Restructuring and removing inconsistencies/duplication and replacing with references to global policies	Martin Pearson
5.4				UK Board