Money Laundering Policy

Last updated 11/02/2026

1. Introduction

1.1. Statement

At Bluesource, we are committed to the highest standard of money laundering and terrorist financing prevention. This includes anti-fraud, anti-corruption and anti-bribery which are covered within their own policy documents. We aim to have adequate and proportionate risk assessment tools specific to financial crime risks, whilst not required to comply in the same way as if we were an FSA ("Financial Services Act") regulated organisation, like some of our customers.

The company understands that it has a responsibility to identify and combat money laundering across a broad spectrum. This includes financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime. Our organisation operates in a transparent environment with assessment, monitoring and reporting at the core of all business functions. We are dedicated to the prevention of financial crime and continue to improve upon existing measures.

1.2. What is money laundering?

Money laundering is the process of taking profits from crime and corruption and transforming them into legitimate assets. It takes criminally derived 'dirty funds' and converts them into other assets so they can be reintroduced into legitimate commerce. This process conceals the true origin or ownership of the funds, and so 'cleans' them. As the Company can potentially receive funds from all over the world, for its goods and services, as well as potentially making global payments, it is exposed to the risk of being unwittingly used to launder funds, although at the time of writing this policy, deemed low risk.

1.3. Purpose

This policy supports the Company in its aim to comply fully with all UK legislation and all relevant overseas legislation in relation to Anti Money Laundering and to ensure it minimises the risk of money-laundering taking place in its operations. For the avoidance of doubt, the Company will not do business with anyone who is or whom it suspects of taking part in any activity, knowingly or unknowingly, which it regards as linked with potential money-laundering.

1.4. Scope

This policy applies to all Company workers (employees, contractors, and subcontractors) who are engaged in financial transactions for or on behalf of the Company. Any failure to adhere to this policy may be dealt with under the Company's disciplinary procedures, as appropriate. Note that any such failure will also expose the individual concerned to the risk of committing a criminal offence under relevant UK or overseas money laundering legislation.

1.5. Legislation

The law concerning money laundering is complex and is increasingly actively enforced. It can be broken down into three main types of offences:

i. the principal money laundering offences under the Proceeds of Crime Act 2002;

ii. the prejudicing investigations offence under the Proceeds of Crime Act 2002; and
iii. offences of failing to meet the standards required of certain regulated businesses, including offences of failing to disclose suspicions of money laundering and failing to comply with the administrative requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

All companies in the UK are required to comply with the Proceeds of Crime Act 2002. Whilst it is not authorised or regulated by the Financial Conduct Authority and therefore does not have to comply with Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, it is considered best practice for the Company to do so.

2. Policy

2.1. Company Requirements

In the UK, severe penalties can be imposed on both the Company and its employees (as individuals) connected with any stage of laundering money and therefore must consider the risks that its business activities will expose it to potential money laundering and devise suitable controls that protect it and its employees against being the victim of money laundering.

These risks need to be documented (**see 2.2 below**) and monitored on a regular basis and must consider how it trains it staff to spot potential signs of money laundering activity and to report it.

When operating overseas, the Company also needs to ensure compliance with local money laundering regulations.

2.2. Areas of risk

Potential risks can exist from the 3 main stages of money laundering:

- **Placement** where the proceeds of criminal activity enter the financial system,
- **Layering** where the money is distanced from its illegal source by being passed through layers of financial transactions, and
- **Integration** where illegal proceeds are reintroduced into legitimate business under seemingly acceptable reasons for the funds.

There are many types of potential risk, with overseas payments often posing a higher risk as they can often be made via a third party, can involve the movement of money through multiple bank accounts or involve high risk countries (**as outlined in 2.3 below**). The Company has identified the following key areas which could be exploited by those trying to carry out any or all the three stages of money laundering, above.

- Receiving fees from overseas
- Receiving funds from potentially criminal business entities
- Making refunds to customers
- Receiving cash transactions (if applicable)
- Receiving donations
- Overseas operations

2.3. Warning signs

It is not possible to give a definitive list of ways to spot money laundering. The following are types of risk factors which may, either alone or collectively, suggest the possibility of money laundering activity:

- A new customer or business partner who is unknown to the Company
- A new customer of business partner who has a bad, low or no credit history
- A customer from a country known to carry a high level of risk (such as a sanctioned country, or a country with known high levels of financial fraud or corruption)
- A secretive person or business, such as those that refuse to provide requested information without a reasonable explanation
- A new customer or business partner who frequently changes their details, such as company name, business address, bank details, etc.
- A request to pay a substantial sum in cash to the Company
- Concerns about honesty, integrity, identity or location of the people involved
- Involvement of an unconnected third party without a logical reason or explanation
- Overpayments for no apparent reason, and requests to pay the difference back to a third party
- Absence of any clear legitimate source for the funds received
- Significant changes in the size, nature, frequency of transactions with a customer that are without reasonable explanation
- Cancellation, reversal, or requests for refunds of earlier transactions
- Requests for account details outside the normal course of business
- A history of poor business records, controls, or inconsistent dealing
- Receipt of a payment for which the Company has not issued an invoice
- A receipt of fees from an unconnected third party
- Any other facts which tend to suggest that something unusual is happening and give reasonable suspicion about the motives of individuals or a company.

2.4. Controls

2.4.1. Due diligence

Due diligence is the process by which the Company assures itself of the provenance of funds it receives and that it can be confident that it knows the people and organisations with whom it works. In this way the Company is better able to identify and manage risk.

Due diligence should be carried out before the funds are received. Funds must not be returned before due diligence has been carried out. In practical terms this means:

i. identifying and verifying the identity of a payee, typically a customer, reseller, or their affiliate;
ii. verify the country of residence and compare against countries known for potential high levels of money laundering, such as using SCHEDULE3ZA of "The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (legislation.gov.uk)";
iii. where the payment is to come from or to be made by a third party on behalf of the intended payee, identifying and verifying the identity of that third party;
iv. identifying and verifying the source of funds from which any payment to the Company will be made; and
v. identifying and in some circumstances verifying the source of funds, such as proof of bank account, etc.

If money laundering is suspected, the Company's Whistle Blowing Policy (see the "**Employee Handbook**" for further details), may be used to flag the concern.

2.4.2. Transactional Controls

The Company has a robust "know your customer" process for customers, partners, and business associates, especially those that are unknown and especially if oversees. Due diligence must be performed during onboarding, including checks that the company has a good credit history, has a been trading for several years and is not on any sanctions lists. The Company's transactional controls include and are not limited to:

- Credit checks performed on new customers via an external credit rating agency prior to being approved, with senior management approval for low credit scores
- Verify which country the money is coming from to satisfy whether it is from a high risk location, prone to potential money laundering
- Proof of accounts and bank accounts where necessary
- No cash is accepted for fees
- Refunds should not be made other than to the original payer
- Unallocated payments purporting to be from customers are returned to source where no registered customer is identified
- Other than in exceptional circumstances, refunds are only made using the original mode of payment and to the same account
- Any potential breaches of this policy must be flagged as outlined below in Section 3 below.

2.4.3. Training

Regulated businesses are required to undertake training relevant for their staff's role and responsibilities to ensure they have the necessary skills to protect the organisation against money laundering and terrorist financing. Whilst the Company is not regulated, many of its customers may be, and as a supplier to them, the Company has a responsibility to ensure that it is also reasonably aware.

On joining the Company, any staff member whose duties will include undertaking a finance function must be made aware of Anti-Money Laundering and their responsibilities to spot, prevent and report such, as part of their induction process. This may include training provided by an online resource, and/or suitably experienced staff. Such anti-money laundering training will include this Policy, the applicable law, an overview on what money laundering is, risks, things to look out for, its link with terrorism, reporting and testing their knowledge.

The Company will retain any training records related to anti-money laundering for at least 5 years.

3. Reporting

3.1. Internal Reporting

It is best practice for the Company to appoint a nominated Senior Manager to be aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing, and if necessary to report it through channels described below. The nominated Senior Manager at the Company is the Head of Operations.

Where a member of staff knows or suspects that money laundering activity is taking, or has taken place, or becomes concerned that their involvement in a transaction may amount to a breach of the regulations, they must disclose this immediately to their line manager or the Company's whistle blowing process (see the "**Employee Handbook**" for further details).

If reasonable suspicion is confirmed it should be communicated to the Head of Operations by email and include as much detail as possible including:

- details of the people, companies or other entities involved, including the individual making the disclosure and other members of staff if relevant
- details of transaction and nature of each person's involvement in the transaction
- suspected type of money laundering activity with exact reasons as to why the individual making the disclosure is suspicious
- the dates of any transactions, where they were undertaken, how they were undertaken and the likely amount of money or assets involved
- any other information that may help judge the case for knowledge or suspicion of money laundering and to facilitate any report to the relevant authorities.

Once this suspicion has been reported to the Head of Operations any instructions provided by the Head of Operations must be followed. Further enquires must not be made unless instructed to do so by the Head of Operations. At no time and under no circumstances should any suspicions be voiced to the person(s) suspected of money laundering. If appropriate the Head of Operations will refer the case to the UK authorities who will undertake any necessary investigation. This may include consent to continue with a particular transaction and care should be taken not to 'tip off' the individuals concerned, otherwise this may be committing a criminal offence. Reports made by a member of staff to the Head of Operations under the above procedures will be considered for treatment as a disclosure.

3.2. External Reporting

On receipt of a disclosure report the Head or Operations will:

- Note the date of receipt and acknowledge receipt of it.
- Assess and advise the individuals concerned when a response can be expected.
- Consider the report and any other relevant information, undertaking further enquiries necessary to decide if a report should be made to the National Crime Agency (NCA).

Once the Head of Operations has evaluated the case a timely determination will be made as to whether:

- There is actual or suspected money laundering taking place.
- There are reasonable grounds to know or suspect that is the case.
- Consent is required from NCA for a particular transaction to proceed.

Where the Head of Operations concludes that the case should be disclosed to NCA this needs to be done:

- In a timely manner, and
- In the prescribed manner on a standard report format provided by NCA.

Where the Head of Operations concludes that there are no reasonable grounds to suspect money laundering then consent will be given for transactions to proceed, and the disclosure report will be marked accordingly.

Details of the reporting to the NCA can be found at: https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities.

4. Monitoring

To enable monitoring to be conducted and compliance with this policy to be evidenced, the Company will retain all anti-money laundering records securely for a period of at least five years.

5. Governance

5.1 Responsibility

The Head of Operations has overall responsibility for this policy and for the effective operation of anti-money laundering procedures. Staff are expected to be familiar with this policy and to contribute to its effective implementation.

5.2 Implementation and Communication

Company workers will be notified of the policy through applicable induction, topic specific training for applicable workers and through the Employee Handbook. The policy will also be available on the policies page of the Company's intranet and externally facing website.

5.3 Exceptions

Any exceptions to this policy require approval from the Head of Operations.

5.4 Review and Update

This policy shall be reviewed and updated from time to time, typically annually or in line with any legislative changes, with a new version created and published accordingly.

.

6. Sign Off

For Bluesource	
Name	Nick Jaggers
Position	Head of Operations
Signature	
Date	11/02/2026

7. Revision History

Revision Date	Reviser	Description of Revision
02/10/2023	Nick Jaggers	Policy created
22/02/2024	Nick Jaggers	Reviewed and rebranded
11/02/2026	Nick Jaggers	Reviewed and no changes needed