Anti-Money Laundering Policy

Anti-Money Laundering Policy Contents

Customer Due Diligence

The business ensures that the identities of all new and existing clients are verified to a reasonable level of certainty. This will include all individual clients, all directors and shareholders with a stake holding of 25% or more of client companies & all partners of client partnerships identities will be verified either online or face-to face or by a combination of both.

Only recognised online identity verification agencies, which use data from multiple sources over a period, will be used (such as Call Credit). These commercial agencies must have processes that allow the enquirer to capture and store the information they use to check and verify an identity.

The following documentation may be presented by the individual:

In person

Either a passport, driver's licence, or government issued document featuring a matching photograph of the individual, and a full name and date of birth matching those provided. An original recent utility bill, or government issued document with the same and address matching those provided by the individual.

Not in person

As in person but additionally:

Any government issued document that provides the date of birth, NI or Tax number or other such government identifier.

Other forms of identity confirmation, such as evidence of a longstanding relationship with the client, or a letter of assurance from independent and reliable persons or organisations, who have dealt with the client for some time, may also provide a reasonable level of certainty. If the business fails to verify the identity of a client with reasonable certainty it will not establish a business relationship or proceed with the transaction. If a potential or existing client either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the business shall refuse to commence a business relationship or proceed with the transaction requested.

Risk Assessment and Ongoing Monitoring

The business shall take a risk-based approach in monitoring the financial activities of its clients. This will be carried out whilst preparing the accounts or tax returns or conducting any other business with the client.

The business will conduct ongoing monitoring of business relationships with customers, to ensure that the documents, date or information held evidencing the customer's identity are kept up to date.

The following are examples of changes in a client's situation that may be considered suspicious:

- A sudden increase in business from an existing customer;
- Uncharacteristic transactions which are not in keeping with the customer's known activities;
- Peaks of activity at locations or at particular times;
- Unfamiliar or untypical types of customer or transaction.

Whenever there is cause for suspicion, the client will be asked to identify and verify the source or destination of the transactions, whether they be individuals or company beneficial owners.

No action need be taken if there is no cause for suspicion.

Monitoring and Managing Compliance

The Data Protection Officer will regularly monitor the following procedures to ensure they are being carried out in accordance with the Anti-Money Laundering policies and procedures of the business:

- Client identity verification;
- Reporting suspicious transactions;
- Record keeping.

The Data Protection Officer will also monitor any developments in the Anti-Money Laundering Regulation and the requirements of the Anti-Money Laundering supervisory body. Changes will be made to the Anti-Money Laundering policies and procedures of the business when appropriate to ensure compliance.

Suspicious Activity Reporting A Suspicious Activity Report (SAR) will be made to the National Crime Agency (NCA) as soon as the knowledge or suspicion that criminal proceeds exist arises.

The Data Protection Officer will be responsible for deciding whether, or not the suspicion of illegal activity is great enough to justify the submission of a SAR.

Further details on National Crime Agency and SARS can be found at http://www.nationalcrimeagency.gov.uk/about-us/what-wedo/economic-crime/ukfiu/how-to-report-sars.

Record Keeping

Records of all identity checks will be maintained for up to 5 years after the termination of the business relationship or 5 years from the date when the transaction was completed. The business will ensure that all documents, data or information held in evidence of customer identity are kept up to date.

Copies of any SAR, together with any supporting documentation filed will be maintained for 5 years from the date of tiling the SAR.

All records will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.