



AML Policy

James Gorey Ltd is committed to ensuring that it has adequate controls to counter money laundering activities and terrorist financing activities, in line with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Risk assessments will be carried out within our policies and procedures to help prevent money laundering and terrorist financing.

This risk based approach is where we assess the risk of customer's laundering money through our business activities. Although we accepted that the majority of our customers will not launder money, we must identify criteria that would indicate a higher risk of money laundering. An example of this is where we do not meet the client face-to-face at any point during the transaction.

As part of mitigating the risk James Gorey Ltd recognises that it is essential for all staff to receive training in anti-money laundering legislation and as such all staff are trained to understand the company's responsibilities and how to identify risk. Each member of staff is also provided with a copy of this Money Laundering Policy as a reminder of their responsibilities and where/how to report suspicious circumstances.

Our nominated Money Laundering Reporting Officer (MLRO) is James Gorey, whose responsibility is to receive internal reports. Our MRLO is then responsible for making a decision as to whether further due diligence is needed, or a report should be made to The National Crime Agency. If it is decided that a report must be made it is the responsibility of our MLRO to file the report with The National Crime Agency (NCA).

Adherence to the "Due Diligence" identification procedures on every occasion will mitigate the risks of the business being used to launder money or fund terrorism. We recognise that under the regulatory guidance we can do this by either taking paper documentation or running an appropriate electronic Anti Money Laundering check.

The regulations identify that "Due Diligence" should be carried out on our "Client" and are required because we deal with one off transactions of €15000 or more. The customer we must identify is the beneficiary of the transaction, identified as anyone who owns or controls 25% or more of the property. Therefore all (Vendors/ Landlords) will be subject to an electronic Anti Money Laundering check. Should the check be unsuccessful we will then seek further identification through approved documentation. Should a face to face meeting not take place or the transaction be one that is identified as high risk by the company then the electronic check will be run through on "High Risk" which will check the client more thoroughly. Again, should this not be successful further identification will be sought through approved documentation.

This policy and our procedures will be reviewed annually to ensure they adequately reflect the risk of money laundering to the company. Where the client is identified by electronic means it is done so to the following guidelines which are stipulated on the regulatory guidance.

Verifying an individual's identity electronically.

If we verify an individual's identity electronically, we should do so from two separate online sources

or a use a service provider that does so. This check must use data from multiple sources collected over period of time or incorporate checks that assess the strength of the information supplier. An electronic check from a single source (for example, a single check against the electoral roll) isn't enough on its own to provide satisfactory evidence of identity.

An electronic record check establishes that an individual exists, not that our customer is that individual. We should therefore verify key facts that only the customer may know to establish who they say they are. To adhere to this guidance we use a Credit Safe money laundering check which in turn uses Experian's data to check multiple data sources. It also allows us to check the client is the individual by verifying their date of birth and time at the address. To get a pass the check must match at least two databases to the client's full name and address. Where the client is seen as high risk we will set the check to high risk, which in turns means matching 3 databases for the check to be verified.

Where we have been unsuccessful in identifying the client electronically, we will collect documents in line with the following which is stipulated by the regulatory guidance.

A government issued document with the customer's full name and photo with either the customer's date of birth or residential address such as:

1. Valid passport
2. Valid photo card driving licence
3. National identity card
4. Firearms certificate

A government issued document (without a photo) which includes the customer's full name and supported by secondary evidence:

1. Old style driving licence
2. Recent evidence of entitlement to state or local authority-funded benefit such as housing benefit, council tax benefit, pension, tax credits

Supported by secondary evidence such as:

1. A utility bill
2. Bank or building society statement
3. Most recent mortgage statement from a recognised lender

For customers other than private individuals

For customers who are not private individuals, such as corporate customers and private companies, the business must obtain information that is relevant e.g. company registration number, registered address and evidence that the individuals have the authority to act for the company – a search at Companies House will reveal details of directors and the Company Secretary. If subsequently we identify a person who has control of/owns 25% or more the business, we will take steps to identify those individuals.

Suspicious Activity Reporting.

WARNING: We will report all suspicious activity to The National Crime Agency (NCA)