Anti-Money Laundering Policy



GENISTAR
Financial Freedom For All

Version Control

Version	Date	Details of Changes	Owner	Changes Made By	Changes Checked By
V1	19/06/2008	Policy Created			
V1.2	01/06/2018	Reviewed and Enhanced	Louise Skilton	Louise Skilton	Louise Skilton
V1.3	31/07/2020	Reviewed and added to new template	Louise Skilton	Louise Skilton	Louise Skilton
V1.4	25/02/2021	Amended by DJ at SB	Elaine Parkes	Elaine Parkes	Elaine Parkes
V1.5	11/05/2021	Reviewed and added to new template	Elaine Parkes	Elaine Parkes	Elaine Parkes

Contents

1. Introduction....1
2. Scope....1
3. What is Money laundering and the Financing of Terrorism?....1
4. The Steps of Money Laundering....1
- 4.1. Examples of Money Laundering....2
- 4.2. Examples of Suspicious Activity....2

5. What are the Money Laundering Offences?....3
- 5.1. Tipping Off....3
- 5.2. Assistance....3
- 5.3. Failure to Report....3
- 5.4. Systems and Controls....3

6. Laws and Regulations....3
- 6.1. What are the Obligations of Genistar?....4

7. Client Due Diligence (CDD)....4
- 7.1. Politically Exposed Persons (PEP)....5
- 7.2. Financial Sanctions....5

8. Anti-Money Laundering Escalation Process....6
9. How Can Money Laundering be Spotted?....7
10. What to do if you Expect Money Laundering....7
- 10.1. Report it to the Money Laundering Reporting Officer (MLRO)....7
- 10.2. Who is the MLRO?....8
- 10.3. What will the MLRO do with a Disclosure?....8

11. Penalties....9
12. Record Keeping Procedures....9
13. Policy Compliance and Audit....9

1) Introduction

1. Genistar is a Financial Services company regulated by the Financial Conduct Authority (FCA).

2. Genistar is currently a low risk company in relation to Money Laundering but it is extremely important that all members of Genistar are familiar with their legal responsibilities. Serious criminal sanctions may be imposed for breaches of the legislation. A key requirement is for members of Genistar to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer (MLRO).

2) Scope

1. This Policy applies to all members of Genistar and aims to maintain the high standards of conduct which currently exist within the business by preventing criminal activity through Money Laundering. The Policy sets out the procedures which must be followed for example, the reporting of suspicions of Money Laundering activity to enable Genistar to comply with its legal obligations.

3) What is Money Laundering and the Financing of Terrorism?

1. Money Laundering is the process of channeling 'bad' money into 'good 'money in order to hide the fact the money originated from illegal activity.

2. Crimes that generate large sums of money, which needs to be laundered, include drug trafficking, theft, terrorism, criminal deception, tax evasion, burglary, handling stolen goods, forgery, extortion and blackmail.

3. Potentially any member of Genistar could be caught by the Money Laundering provisions if they suspect Money Laundering and either become involved with it in some way and/or do nothing about it. This policy sets out how any concerns should be raised.

4) The Steps of Money Laundering

1. Money laundering is not a single act but is a process that is accomplished in three basic steps.

Step 1 - Placement:

This is the first stage of the process and usually involves the placing of large sums of cash into the financial system, the retail economy or out of the country. The aim is to remove the cash from the location of acquisition to avoid detection by the authorities and to transform it into other assets, i.e. to buy high value goods, property or business assets.

Step 2 - Layering:

This is the attempt at concealing or disguising the source of the funds by creating complex layers of financial transactions designed to disguise the audit trail. Its aim is to disassociate the illegal monies from the source of the crime by creating a complex web of financial transactions aimed at concealing the source and ownership of the funds, i.e. wire transfers abroad often using shell companies or funds disguised as proceeds of legitimate business, cash deposited in overseas banking system and the resale of goods/assets.

Step 3 - Integration:

This final stage is when the money is integrated into the legitimate economic and financial system. This integration is accomplished by the launderer making it appear that the money has been legally earned i.e. false loan repayments or forged invoices, complex web of transfers both domestic and international, so that tracing of original sources is almost impossible and income from property or legitimate business assets appears clean.

4.1. Example of Money Laundering

Illegal cash is used (placed) to pay for the annual non-domestic rates on a commercial premise (possibly also large overpayment), and then within a very short time the property is vacated (layering). A refund is made to the individual from the Council, (integrating) the source of the money.

4.2. Examples of Suspicious Activity

1. A suspect could be a client, an agent or a member of Genistar. The following examples highlight situations that may give rise to suspicion of Money Laundering:

- An intention to settle fees by cash
- A request by a client to enter into a mortgage contract(s) where, the source of the funds to repay the loan is unclear or not consistent with the client's apparent standing
- A proposal that has no discernible purpose and a reluctance to divulge a 'need'
- A request to repay large amounts of outstanding capital
- Regular cash payments to repay outstanding capital
- An intention to pay fees by utilising a cheque drawn other than from the personal account of the proposer
- The money laundering regulations cover tax evasion. If a client states; that there is a difference between actual income and reported income, then any suspicion that the additional funds are being used as a large deposit to purchase a property should be reported
- The client who is based in the UK and seeks to pay fees or repay capital by unusual means, which appears to be attempting to by-pass money laundering controls
- The client who is introduced by an overseas agent, an affiliate of another company that is based in a country where the production of drugs or drug trafficking may be prevalent, for example, South America or South East Asia

- Requests to transfer funds overseas and make payments with foreign currency
- Applications in different names but with common addresses
- The use of an address that is not the client's permanent address
- Several mortgage applications with common references, addresses, valuers, agents, solicitors, etc.
- Mortgage applications with unusually high earning figures, especially if taking advantage of 'self-certification'.

5) What are the Money Laundering Offences?

5.1. Tipping Off

1. Tipping off is where someone informs a person or people who are, or are suspected of being involved in Money Laundering, in such a way as to reduce the likelihood of them being investigated.

5.2. Assistance

1. The laws governing the responsibilities of financial institutions with regards to AML/Terrorist Financing (TF)put a personal responsibility on all Intermediaries and their members/staff. The following offences are punishable:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the 2002 Act)
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328)
- Acquiring, using or possessing criminal property (section 329)
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorist Act 2000).

5.3. Failure to Report

1. It is an offence not to report the knowledge or suspicion of money laundering as soon as is reasonably practical after the information comes to your attention.

5.4. Systems and Controls

1. It is also a separate offence under the AML Regulations not to have systems and procedures in place to combat money laundering (regardless of whether or not money laundering actually takes place).

6) Laws and Regulations

1. On 20th December 2019, new legislation came into place, which was driven by the Fifth Money Laundering Directive. This new legislation sets out the amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). The new provisions came into force in national law on 10 January 2020.

2. The principal legislation and regulations enacted to combat Money Laundering are:

- The Money Laundering Regulations 2007
- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
- The Proceeds of Crime Act (POCA) 2002
- The Terrorism Act 2000
- Financial Services and Markets Act 2000 (FSMA)
- Joint Money Laundering Steering Group (JMLSG)

6.1. What are the Obligations of Genistar?

1. Genistar is required to identify and monitor clients on a risk sensitive basis and follow the guidance set out by the Joint Money Laundering Steering Group (JMLSG). Anyone transacting into business with Genistar must be subject to a form of risk based due diligence.

2. Genistar has a duty to ensure the following are in place:

- Appoint a Money Laundering Reporting Officer ("MLRO") to receive disclosures from members of Genistar of Money Laundering activity
- Maintain client identification procedures
- Maintain record keeping procedures
- Implement a disclosure procedure to enable the reporting of suspicions of Money Laundering
- Identify the money laundering and terrorist financing risks that are relevant to the business
- Design and implement controls to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls

7) Client Due Diligence (CDD)

1. Where Genistar undertakes activities of onboarding, Client Due Diligence must be carried out before any business is undertaken.

2. Genistar needs to know who their customers are to guard against fraud, including impersonation fraud and the risk of committing offences under POCA and the Terrorist Act relating to Money Laundering and Terrorist Financing.

3. Genistar are required to identify individuals and, where applicable, beneficial owners. It must then verify these identities. Information on the purpose and intended nature of the business relationship must also be obtained. The firm must then conduct ongoing monitoring of the business relationship.

4. The aim of the CDD is to identify the different types of individuals and to establish their identity. This includes both their name and address. It must be noted that failure to keep records of the verification process is considered a serious offence.

5. Any member of Genistar who knowingly confirms an individual's identity with incorrect verification details, may be committing a criminal offence. This would include incorrect confirmation by a member of Genistar that ID (e.g., Passport or driver's licence) had been seen when only a photocopy was actually looked at.

6. Due diligence will be carried out in two distinct parts; verifying a client's identity (CDD) and, where the riskbased assessment has highlighted a higher risk, additional information will need to be gathered under Enhanced Due Diligence (EDD) of Know your Customer (KYC).

7.1. Politically Exposed Persons (PEP)

1. A PEP is defined as an individual who is entrusted with prominent public functions. Following the new requirements introduced under the Fourth Money Laundering Directive, the additional requirements for PEPs are extended to their immediate family or close associates.

2. The following UK functions will be treated as prominent public functions:

- Members of the UK government, and members of the devolved administrations in Scotland, Wales and Northern Ireland
- Members of the UK Parliament, and members of the Scottish Parliament, Welsh Assembly and Northern Irish Assembly
- Members of the national governing bodies of political parties represented in any of the UK Parliament, Scottish Parliament, Welsh Assembly and Northern Irish Assembly.
- Justices of the UK Supreme Court
- Members of the Court of the Bank of England
- Ambassadors, Permanent Secretaries/Deputy Permanent Secretaries
- Board members of for-profit enterprises in which the state has an ownership interest of 50% or more, or where reasonably available information points to the state having control over the activities of the enterprise
- Directors, Deputy Directors, and board members of international public organisations headquartered in the UK

3. While PEP status does not incriminate individuals or entities, it may put a client into a higher risk category and enhanced due diligence should be undertaken.

4. Genistar perform an electronic background check on all individuals which will flag if someone is classified as a PEP.

7.2. Financial Sanctions

1. The Financial Sanctions order prohibits a firm from carrying out transactions with certain people or organisations (known as targets). In some cases, the order will prohibit a firm from providing any Financial Services to the target.

2. Genistar are required to check the Financial Sanctions List for ALL individuals to ensure they do not deal with any individuals whose details have been included in the Financial Sanctions List.

3. HM Treasury (HMT) maintains a list of targets, known as the UK Consolidated Financial Sanctions List (HMT list). A breach of a Financial Sanctions order may be a criminal offence. The full list can be located on the HMT website.

4. Genistar perform an electronic background check on all individuals which will flag if someone is classified as having a Financial Sanction. Where any individual is found to be on the HMT list, Genistar must immediately stop the provision of any service and report the matter, as soon as possible, to HMT's Asset Freezing Unit.

8) Anti Money Laundering Escalation Process

All Genistar representatives and staff members have a responsibility to follow the AML client verification process prior to any new business application be submitted / processed. The escalation process should be followed in the event of an AML alert has been triggered.

Key Confirmation

- Client consent for agent / representative to conduct an electronic verification search (Smart Search).

Smart Search Submission

- Submit Smart Search
- If Smart Search verification is successful proceed with application.
- If Smart Search is unable to verify the client, the agent / representative to gather additional supporting documentation to verify client.
- If Smart Search triggers a potential AML alert
- Case to be referred to the Business Integrity Team (Enhanced Due Diligence).

Enhanced Due Diligence

- The Business Integrity team to investigate AML alert i.e. Sanctions, PEPs, Occupation Hits or Adverse Media
- If the investigation identifies the alert to be legitimate, then application to be cancelled and AML register to be updated.
- If the alert has been discounted, due diligence to gathered and stored on the client file.

Gathering Additional Information

- Business Integrity to reset the application and request additional documentation in order to verify the client's identity.
- Client Verification - Passport & Drivers Licence
- Address Verification – Recent Bank Statement, Utility Bill (dated within the last 3 months) Council Tax Bill & Tax Assessment documents.
- If unable to satisfy client verification or proof of residency, application to be cancelled and AML register to be updated.
- Once ID has been attained, Business Integrity to re-run SmartSearch check. If ID check passes, Business Integrity will update register.

Application to Proceed

- Upon successful sign off, proceed with application.

Application to Proceed

- Upon successful sign off, proceed with application which will then go to Submissions to process.

9) How Can Money Laundering Be Spotted?

1. It is not possible to provide an exhaustive list of the ways to spot money laundering or state every scenario in which you should be suspicious, however, the following, are examples of possible "indicators of suspicion" for money laundering activity:

- Transactions which have no apparent purpose, and which make no obvious economic sense
- Where the transaction being requested by the client, without reasonable explanation, is out of the ordinary range of services normally requested or is outside the experience of the firm in relation to the particular client
- Where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged
- Where the client refuses to provide the information requested without reasonable explanation
- Where cash has been tendered which significantly, exceeds the amount of the debt
- Where a debt has been paid twice or more and a refund of the balance been requested
- Where a client who has entered into a business relationship uses the relationship for a single transaction or for a very short period of time
- The extensive use of offshore accounts, companies, or structures in circumstances where the client's needs do not support such economic requirements
- Unnecessary routing of funds through third-party accounts
- Unusual investment transactions without an apparently discernible profitable motive

10) What to do if you Suspect Money Laundering?

10.1. Report it to the Money Laundering Reporting Officer (MLRO)

1. You should report any suspicious transactions or concerns as soon as practicable to the MLRO using the Suspicious Activity Report (SAR). This must be done immediately.

2. You should also report any complaints you receive from a member of the public in relation to possible criminal activity being carried out by someone who may be a customer of Genistar.

3. Once you have reported the matter to the MLRO, you must follow any directions given to you by the MLRO. You must NOT make any further enquiries into the matter yourself. The MLRO will consider the report and any necessary investigation will be undertaken by the Proceeds of Crime Act 2002 (POCA). All members of Genistar will be required to co-operate during any subsequent Money Laundering investigation.

4. Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of Money Laundering, even if the NCA has given consent to a particular transaction proceeding. If you do, you may commit a criminal offence of "tipping off" which may render you liable to prosecution.

5. Do not, therefore, make any reference on a client file to a suspicious transaction report having been made to the MLRO. Should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

10.2. Who is the MLRO?

1. Genistar's Money Laundering Reporting Officer is: Mark Kecek

2. A suspicious activity report can be sent to: business.integrity@genistar.net or via post to the address below:

FAO: Money Laundering Reporting Officer
Genistar Limited
Victoria House
Harestone Valley Road
Caterham
CR3 6HY

10.3. What will the MLRO do with a Disclosure?

1. Upon receipt of a suspicious transaction report, the MLRO must note the date of receipt on the relevant section and acknowledge receipt of it. The MLRO will advise the person making the disclosure of the timescale within which they expect to respond.

2. The MLRO will consider the report and any other relevant information in order to ensure that all available information is taken into account in deciding whether a report to the National Crime Agency (NCA) is required (such enquiries being made in such a way as to avoid any appearance of 'tipping off' those involved).

3. Only the MLRO will contact the NCA.

4. Other relevant internal information may include:

- Reviewing other transaction patterns and volumes
- The length of any business relationship involved
- The number of any one-off transactions and linked one-off transactions
- Any identification evidence held

5. The MLRO may also need to discuss the report with the person making the disclosure.

6. Once the MLRO has evaluated the suspicious activity report and any other relevant information, a decision will be made as to whether:

- There is actual or suspected money laundering taking place; or
- There are reasonable grounds to know or suspect that is the case; and
- Whether there is the need to seek consent from the NCA for a particular transaction to proceed.

7. Where the MLRO does so conclude, then the matter must be disclosed as soon as practicable to the NCA. This can be reported using their preferred reporting method electronically on "SAR Online".

8. Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question must not be undertaken or completed until the NCA has specifically given consent, or there is deemed consent through the expiration of the relevant time limits without objection from the NCA.

9. Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then the report will be marked accordingly, and consent given for any on-going or imminent transaction(s) to proceed.

10. The MLRO must maintain records of reports received and disclosures made, so that they may be used as evidence in any subsequent investigation by appropriate agencies. The records must be capable of providing an audit trail that identifies the individual and the relevant transaction/suspicion.

11) Penalties

1. Money laundering offences may be tried at a magistrate's court or in the Crown Court, depending on the severity of the suspected offence.

2. In a Crown Court, fines are unlimited and with possible prison sentences of between two to 14 years.

- Assistance – up to 14 years imprisonment and/or fine
- Failing to report – up to 5 years imprisonment and/or fine
- Tipping off – up to 5 years imprisonment and/or a fine

12) Record Keeping Procedures

1. Legislation requires that records of any evidence obtained in support of the identification of a client along with details of all relevant business transactions with the client must be kept on file for five years after the end of the business relationship.

2. Upon the expiry of the 5 years period, personal data must be deleted unless:

- The firm is required to retain it under enactment of any court proceedings
- The data subject has given express permission for you to retain it
- The firm has a legitimate interest or legal obligation to continue to hold the data for example for PI insurance purposes

13) Policy Compliance Audit

1. Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an individual liable to further investigation by the Business Integrity Department which may result in disciplinary or dismissal.

2. Non-compliance with this policy could have a significant effect on the efficient operation of Genistar and may result in financial loss and an inability to provide necessary services to our customers. Genistar will audit its procedures and where practical and proportional.

3. It is the duty of all individuals to report, as soon as practicably possible, any actual or suspected Money Laundering.

4. Any individual who does not understand the implications of this policy or how it may apply to them, should seek advice from their upline and/or the Business Integrity Department.

GENISTAR
Financial Freedom For All

Anti-Money Laundering Policy

GENISTAR LIMITED
Victoria House, Harestone Valley Road, Caterham CR3 6HY
Telephone: +44 (0)20 3372 5085
Authorised and Regulated by Financial Conduct Authority.