Gold Crystal Group Ltd

KYC & AML POLICY

788-790 Nathan Road, Mongkok, Kowloon, Hong Kong
Registration Number 2243184

Scope of policy

This policy applies to all GCGL officers, employees, appointed producers and products and services offered by OctaFX. All business units and locations within GCGL will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location has implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions. All efforts exerted will be documented and retained. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

The committee shall

- Receive internal reports of (suspicions of) money laundering
- Investigate reports of suspicious events
- Make reports of relevant suspicious events to the relevant authorities
- Ensure the adequacy of arrangements made for the awareness and training of staff and advisers
- Report at least annually to the firm’s governing body on the operation and effectiveness of the firm’s systems and controls.
- Monitor the day-to-day operation of anti-money laundering policies in relation to: the development of new products; the taking on of new customers; and changes in the firm’s business profile.

Policy

It is the policy of GCGL to actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. GCGL is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.

For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

What is Money Laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for “clean” money or other assets with no obvious link to their criminal origins.

Criminal property may take any form, including money or money’s worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property

- Entering into arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

There is no single stage of money laundering; methods can range from the purchase and resale of luxury items such as a car or jewellery to passing money through a complex web of legitimate operations. Usually the starting point will be cash but it is important to appreciate that money laundering is defined in terms of criminal property. This can be property in any conceivable legal form, whether money, rights, real estate or any other benefit, if you know or suspect that it was obtained, either directly or indirectly, as a result of criminal activity and you do not speak up then you too are taking a part in the process.

The money laundering process follows three stages:

1. Placement

   Disposal of the initial proceeds derived from illegal activity e.g. into a bank account.
2. Layering

   The money is moved through the system in a series of financial transactions in order to disguise the origin of the cash with the purpose of giving it the appearance of legitimacy.
3. Integration

   Criminals are free to use the money as they choose once it has been removed from the system as apparently “clean” funds.

No financial sector business is immune from the activities of criminals and Firms should consider the money laundering risks posed by the products and services they offer.

What is Counter Terrorist Financing (CTF)?

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organisations for ideological, political or other reasons. Firms must therefore ensure that: (i) customers are not terrorist organisations themselves; and (ii) they are not providing the means through which terrorist organisations are being funded.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Risk Based Approach

The level of due diligence required when considering anti-money laundering procedures within the firm, it should take a risk-based approach. This means the amount of resources spent in conducting due diligence in any one relationship that is subject risk should be in proportion to the magnitude of the risk that is posed by that relationship.

These can be broken down into the following areas:

Customer Risk

Different customer profiles have different levels of risks attached to them. A basic Know your Customer (KYC) check can establish the risk posed by a customer. For example, near-retired individuals making small, regular contributions to a savings account in line with their financial details poses less of a risk than middle-aged individuals making

ad-hoc payments of ever-changing sizes into a savings account that does not fit into the profile of the customers' standing financial data. The intensity of the due diligence conducted on the latter would be higher than that carried out on the former as the potential threat of money laundering in the second case would be perceived as being greater. Corporate structures can be used as examples of customers that could carry a higher risk profile than the one just seen, as these can be used by criminals to introduce layers within transactions to hide the source of the funds, and like that, clients can be categorised into different risk bands.

Product Risk

This is the risk posed by the product or service itself. The product risk is driven by its functionality as a money laundering tool.

The Joint Money Laundering Steering Group has categorised the products with which Firms typically deal into three risk bands – reduced, intermediate and increased. Typically, pure protection contracts are categorised as reduced risk and investments in unit trusts as increased risk. Additionally, a factor that will contribute to the classification of the risk category is sales process associated with the product. If the transaction in the product takes place on an advisory basis as a result of a KYC, this will carry less risk than an execution only transaction, whereby you know significantly less about the customer.

Country Risk

The geographic location of the client or origin of the business activity has a risk associated with it, this stems from the fact that countries around the globe have different levels of risk attached to them.

A firm would determine the extent of their due diligence measure required initially and on an ongoing basis using the above four risk areas.

Customer Identification Program

GCGL has adopted a Customer Identification Program (CIP). GCGL will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results.

Notice to customers

GCGL will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

Know your customer

When a business relationship is formed, in order to establish what might constitute normal activity later in the relationship, it is necessary for the company to ascertain the nature of the business a client expects to conduct.

Once an on-going business relationship has been established, any regular business undertaken for that customer can be assessed against the expected pattern of activity of the customer. Any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.

Information regarding a client’s income, occupation, source of wealth, trading habits and the economic purpose of any transaction is typically gathered as part of the provision of advice. At the start of the relationship personal information is also obtained, such as,

nationality, date of birth, and residential address. These pieces of information should also be considered in respect to the risk of financial crime (including AML and CTF). For high risk transactions, it might be appropriate to seek verification of the information the client has provided.

Source of Funds

When a transaction takes place, the source of funds, i.e. how the payment is to be made, from where and by who, must always be ascertained and recorded in the client file (this would usually be achieved through retaining a copy of the cheque or direct debit mandate).

Identification

The standard identification requirement for customers who are private individuals are generally governed by the circumstances relating to the customer and the product type that is being dealt in, i.e. the level of risk attributed to the product whether it is a reduced risk, intermediate risk or an increased risk product. Taking that into account for reduced risk and intermediate risk products the following pieces of information are required as a standard for identification purposes:

- Full Name
- Residential Address

Verification

Verification of the information obtained must be based on reliable and independent sources – which might either be documents produced by the customer, or electronically by the firm, or by a combination of both. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification.

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

If the identity is to be verified from documents, this should be based on:

Either a government issued document which incorporates:

- The customer's full name, and
- Their residential address

Photographic Government Issued Identity Documents

- Valid passport
- National Identity card

Alternatively, this can be done by a non-photographic government issued document which incorporates the customer's full name, supported by a second document, which incorporates:

- The customer's full name, and

- Their residential address

Evidence of Address

- Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm (but not ones printed off the internet and not less than 3 months old)
- Utility bills (not including mobile phone bills, not ones printed off the internet and not less than 3 months old)

For increased risk level products, in addition to obtaining the standard information detailed above, the following know your customer information should be obtained and recorded:

- Employment and income details
- Source of wealth (i.e. source of the funds being used in the transaction)

Monitoring and reporting

Transaction based monitoring will occur within the appropriate business units of OctaFX. Monitoring of specific transactions will include but is not limited to transactions aggregating $5,000 or more and those with respect to which GCGL has a reason to suspect suspicious activity. All reports will be documented.

Suspicious activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Examples of red flags are:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer's account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

Know your customer - the basis for recognising suspicions

A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that

type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

Questions you must consider when determining whether an established customer’s transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer’s business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

Suspicious scenarios

Issues which should lead you to have cause for suspicion would include:

- Clients who are reluctant to provide proof of identity;
- Clients who place undue reliance on an introducer (they may be hiding behind the introducer to avoid giving you a true picture of their identity or business);
- Requests for cash related business, for example questions about whether investments can be made in cash, suggestions that funds might be available in cash for investment;
- Where the source of funds for investment is unclear;
- Where the magnitude of the available funds appears inconsistent with the client’s other circumstances (i.e. the source of wealth is unclear). Examples might be students or young people with large amounts to invest;

- Where the transaction doesn't appear rational in the context of the customer's business or personal activities. Particular care should be taken in this area if the client changes their method of dealing with you without reasonable explanation;
- Where the pattern of transactions changes;
- Where a client who is undertaking transactions that are international in nature does not appear to have any good reason to be conducting business with the countries involved (e.g. why do they hold monies in the particular country that the funds are going to or from? Do their circumstances suggest that it would be reasonable for them to hold funds in such countries?);
- Clients who are unwilling to provide you with normal personal or financial information, for no apparent or rational reason. (Care should be taken not to include all distance relationships as suspicious, because most will be for genuine reasons. Suspicions will ordinarily be based upon cumulative as opposed to stand alone issues)

A money launderer is likely to provide persuasive arguments about the reasons for their transactions. Those should be questioned to decide whether a transaction is suspicious.

Reporting a Suspicion

Where, for whatever reason, we suspect that a client, or anybody for whom they are acting, may be undertaking (or attempting to undertake) a transaction involving the proceeds of any crime it must be reported as soon as practicably possible and in writing.

Internal reports must be made regardless of whether any business was, or is intended to be, actually written.

Investigation

Upon notification to the AML Compliance Committee an investigation will be commenced to determine if a report should be made to the appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file the SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

Freezing of Accounts

Where we know that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen.