ANTI-MONEY LAUNDERING POLICY, PROCEDURE AND INTERNAL CONTROL RULES OF

FROGTECH SOLUTIONS DMCC

Registration Number: DMCC188733

Legal address: Unit No: 4107
DMCC Business Centre
Level No 1
Jewellery & Gemplex 3
Dubai
United Arab Emirates

These Rules are based on:

*Central Bank of the UAE Regulations 24/2000, subsequent amendments and changes.

*FATF 40 Recommendations

*Federal Decree-law No. (20) of 2018 ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND FINANCING OF ILLEGAL ORGANISATIONS

*Cabinet Decision No. (10) of 2019 CONCERNING THE IMPLEMENTING REGULATION OF DECREE LAW NO. (20) OF 2018 ON ANTI- MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

*DMCC AML/CFT Guidance for members

The Rules are introduced to all employees of FROGTECH SOLUTIONS DMCC whose duties include establishment of business relationship or carrying out transactions and their monitoring.
FROGTECH SOLUTIONS DMCC shall regularly check whether the Rules are up-to-date and make necessary changes upon amendments to the regulations in force.

OBJECTIVES OF AML/CDD/CFT POLICY

The objective of this policy is to ensure that the products and services of the Company are not used to launder the proceeds of crime and that all of the Company's staff is aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing. The document also provides a framework to comply with applicable laws, Regulatory guidelines specially related with detection and reporting of suspicious activities.

MONEY LAUNDERING

Definition: Money Laundering is the criminal practice of processing ill-gotten gains or "dirty" money, through a series of transactions, in this way the funds are "cleaned" so that they appear to be the proceeds from legal activities, it is also the process to change the identity of illegally obtained money by using banking channel so that it appears to have originated from a legitimate source.

STAGES OF MONEY LAUNDERING

Money laundering can be a diverse and often complex process. The first step in the laundering process is for criminals to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. The funds can further be transferred to other accounts, locally or internationally or use it to buy other goods or services. It eventually appears to be like legally earned money and becomes difficult to trace back to its criminal origin. The criminals can then invest or spend it or, as is often the case, use it to funded more crime.

The laundering process is often described as taking place in three stages:

1. Placement

2. Layering

3. Integration.

1. Placement

The first stage is referred to as Placement. At this stage Illegal funds or assets are first brought into the financial system. When illegal funds are placed in the financial system, they become more liquid. There are numerous Placement techniques, including the following:

*Smurfing

*Alternative Remittances

*Electronic Transfers

*Asset Conversion

*Bulk Movement

*Securities Dealing

Smurfing: involves the deposit of small amounts of illegal cash into account(s). Typically, smurfing deposits are in small amounts in order to avoid Regulatory requirements of reporting cash transactions '

Alternative Remittances: It refers to the transfer of funds through 'alternative' or illegal money transfer system. These systems are unregulated and illegal, but they are used to transfer both legitimate and illegal funds. Alternative Remittances also goes by the names of underground or parallel banking. There are very large networks of these systems in operation around the world.

Electronic Transfers: In the money laundering context, an electronic transfer involves the transfer of money through electronic payment systems that do not require sending funds through a bank account. If the amount is below the CTR (Cash Transaction Reporting) limit then it will not be reported as per prevailing regulations.

Asset Conversion: Asset Conversion simply involves the purchase of goods. Illegal money is converted into other assets, such as real estate, diamonds, gold and vehicles, which can then be sold and proceeds can be deposited in the account.

Bulk Movement: involves the physical transportation and smuggling of cash and monetary instrument such as money orders and checks.

Securities Dealing: Illegal funds are placed with securities firms which is used for buying bearer securities and other easily transferable instruments

2. Layering

Layering is the second stage of money laundering. In this stage illegal funds or assets are moved, dispersed and disguised to conceal their illegal origin. There are numerous techniques and institutions that facilitate layering, including the following:

* Offshore Banks

* Shell Corporations

* Trusts

* Walking Accounts

* Intermediaries

Offshore Banks: Offshore Banks accept deposits from non-resident individuals and corporations. A number of countries have well-developed offshore banking sectors; in some cases, combined with loose anti- money laundering regulations.

Shell Corporations: A Shell Corporation is a company that is formally established under applicable corporate laws, but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold accounts and assets to disguise their actual ownership.

Trusts: Trusts are legal arrangements for holding specified funds or assets for a specified purpose. These funds or assets are managed by a trustee for the benefit of a specified beneficiary or beneficiaries. Trusts can act as layering tools as they enable creation of false paper trails and transactions. The private nature of trusts makes them attractive to money launderers.

Walking Accounts: A Walking Account is an account for which the account holder has provided standing instructions that upon receipt all funds should be immediately transferred into one or more accounts. By setting up a series of walking accounts, criminals can automatically create several layers as soon as any fund transfer occurred.

Intermediaries: Lawyers, accountants and other professionals may be used as Intermediaries or middlemen between the illegal funds and the criminal. Professionals engage in transactions on behalf of a criminal client who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.

3. Integration

Integration is the third stage of money laundering process. In this stage, illegal funds are successfully legitimized by mixing with legitimate funds in the financial system. There are various Integration techniques, including the following:

* Import /Export Transactions

* Business Recycling

* Asset Sales & Purchases

* Consultants

* Credit & Debit Cards

* Corporate Financings

Import /Export Transactions to bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well.

Business Recycling

Legitimate businesses also serve as conduits for money laundering. Cash-intensive retail businesses, real estate, jewelers, and restaurants are some of the most traditional methods of laundering money. This technique combines the different stages of the money laundering process.

Asset Sales & Purchases

This technique can be used directly by the criminal or in combination with shell corporations, corporate financings and other sophisticated means. The end result is that

the criminal can treat the earnings from the transaction as legitimate profits from the sale of the real estate or other assets.

Consultants

The use of consultants in money laundering schemes is quite common. The consultant could be fake. For example, the criminal could himself be the consultant. In this case, the criminal is channeling money back to himself. This money is declared as income from services performed and can be used as legitimate funds.

Credit & Debit Cards:

Credit cards are an efficient way for launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence.

Debit Cards Individuals first transfer illegal funds into an offshore account and also signs up for a debit card from the bank to utilize the funds.

Corporate Financings

Corporate financings are typically combined with a number of other techniques, including use of offshore banks, electronic funds transfers and shell corporations.

The three basic stages may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap.

SOURCES OF MONEY LAUNDERING:

Money laundering may not just involve wealth related to Drug Trafficking / Terrorism financing. List of crimes identified by Financial Action Task Force (FATF) as generators of criminal wealth also included:

1. Illegal arms sales

2. Gun running

3. Organized crime including drug trafficking and prostitution

4. Embezzlement

5. Smuggling (including movement of nuclear materials)

6. Counterfeiting (including making of imitation and copies of original products/goods)

7. Fraud, especially computer-supported fraud

8. Benefiting from insider trading.

9. Bribery and kickbacks

10.Tax evasion

11.Under and over-invoicing of trade transactions.

12.Bogus trade transactions to launder money through round-tripping

13.Facilitating illegal immigration

14.Real Estate Transactions

TERRORIST FINANCING

Terrorist Financing can be defined as the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

THE NEED TO COMBAT MONEY LAUNDERING (ML) AND TERRORIST

FINANCING (TF)

The prevention of ML and TF from the point of view of the Company has three dimensions:

* Ethical - taking part in the prevention of crime.

* Professional - ensuring that the Company is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and, if fraud is involved, its solvency.

* Legal - complying with Laws and Regulations that impose a series of specific obligations on financial services and their employees. The need also arises due to the severe nature of consequences of ML and TF. Following are some examples:

- Unexplained changes in supply and demand for money,

- Contamination of legal financial transactions,

- Systemic risk,

- Unlawful enrichment by perpetrator of crime,

- Weakening of the social, collective ethical standards,

- Drug trafficking, Human trafficking,

- Political corruption,

- Terrorism crimes cause a great deal of human misery.

REGULATORY OVERSIGHT & COMPLIANCE RISKS

FROGTECH SOLUTIONS DMCC has used Central Bank of the UAE Regulations 24/2000, subsequent amendments/changes, UAE and DMCC applicable laws and the best practices and recommendation, to formulate its own AML/CDD/CFT Policy. The consequence of contravening the Regulations or failing to comply can be significant and

include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation for the company.

Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect the company from the following risks:

- Reputational
- Operational
- Legal
- Financial

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong AML/CDD/CFT policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML/CDD/CFT policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Legal risk: If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Financial risk: If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve money that the customer owes.

CUSTOMER DUE DILIGENCE(CDD)

Customer due diligence is a complex of procedures that helps us to establish customer's identity, the nature of the business, intentions for future relationships and compliance with the data provided. The purpose of CDD is to prevent the use of illegally obtained assets and property in the economic activity of the Company. CDD is based, first and foremost, on applying the KnowYour-Customer ("KYC") principle, under which a customer shall beidentified and respective transactions shall be assessed based on the customer's expected business activity. In addition, CDD serves to identify unusual circumstances in the customer's activity whereby an employee of the Company has reason to suspect, or has a knowledge based on facts regarding money laundering or terrorist financing.

In accordance with DMCC recommendations, we should undertake due diligence in the following cases:

▪ establishing the business relationship;

▪ carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;

▪ carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding AED 3,500;

▪ where there is a suspicion of Money Laundering, Terrorist Financing;

▪ where there are doubts about the veracity or adequacy of previously obtained customer's identification data;

▪ on an annual basis;

▪ at periodic intervals based on company status and circumstances.

We adopt a risk based approach to determine the extent of additional due diligence measures with the level of risk posed by the customer type, business relationship, transaction, product/service or geographical location.

Risk factors:

Risk category	Risk Factor
Client risk (for Directors, UBO's and other managers and shareholders of the entity)	*Whether the person is subject to international sanctions (UN, EU, OFAC, etc.). *Whether the person is a politically exposed person[1] ("PEP"). *Whether the person is represented by a legal person (e.g. introducer, attorney). *Whether a third party (individual) is the beneficial owner of the transaction.

	*Circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other persons. *The duration of the operations and the nature of business relationships. *The type and nature of the services used or products consumed by the person outside the Company. *The nature of the personal activities of an individual. *Whether the origin of the person's wealth or the source and origin of the funds used for a transaction can be easily identified.
Client risk (for legal entities)	*Turnover of the customer base *Whether the person's customer base has increased rapidly. *Whether the person provides its services to anonymous customers. *The legal form, management structure, field of activity of the person, including whether it is a trust fund, civil law partnership or another similar contractual legal entity or a legal person with bearer shares. *Whether the identification of the beneficial owner is impeded by complex and nontransparent ownership structure. *Whether the service or product may be related to criminal activity. *Nominal shareholders, directors, selfdeclared ultimate beneficial owners.
Product/ Service risk[2]	*Nature of services provided to the

	customer. *Individual / account type transaction limits.
Geographical risk[3]	*Whether the country applies legal provisions that are in compliance with the international standards of prevention of money laundering and terrorist financing. *Whether there is a high crime rate (incl. drug-related crime rate) in the country. *Whether the known organised crime groups exploit the country to pursue their operations. *Whether the country engages in proliferation of weapons of mass destruction. *Whether there is high level of corruption in the country. *Whether international sanctions have been or are being imposed on the country. *Whether other measures have been taken against or positions of international organizations have been expressed on the country.
Interface / Delivery channel risk	Whether the person has been identified face-to-face or remotely.

[1] Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to the Company as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates. More info listed below.

[2]The Company would not do business with entities that provide such activities:

*Collecting donations as a charity or non-profit organization, NGO's
* Dating *(newly incorporated, not known*);
* Drug paraphernalia - product or accessory that is intended or modified for making, using, or concealing drugs, typically for recreational purposes;
* Drugs / Illicit substances, steroids and certain controlled substances or other products that present a risk to consumer safety;
* Encourage, promote, facilitate or instruct others to engage in illegal activity;
* Extractive Industries;

* High Risk File hosting / sharing and cyberlockers;
* Infringe any duly registered copyrights/trademarks or other violation of intellectual property rights;
* Unregulated pharmaceuticals, illegal drugs and or unlicensed drug related activity;
* Involve offering or receiving payments for the purpose of bribery or corruption any form of high yield financial investments (get rich quick schemes);
* Items that encourage, promote, facilitate or instruct others to engage in illegal activity;
* Oil & Gas Industries;
* PC Support sold via outbound telemarketing;
* Pyramid or Ponzi schemes;
* Relate to the sale of dangerous or hazardous goods;
* Replicas;
* Sale of government ID's or documents;
* Services associated with prostitution, escort;
* Stolen goods including digital and virtual goods (fictitious social media likes, spam emails);
* Unlicensed lottery and gambling;
* Unregulated crypto companies;
* Unregulated Forex;
* Violate any law, statute, ordinance or regulation;
* Weapons, firearms and ammunitions;

[3]The Company would not do business with entities and individuals from such countries:

Afghanistan, El Salvador, Mali, Sierra Leone, American Samoa, Equatorial Guinea, Moldova, Somalia, Aruba, Eritrea, Myanmar, Sudan, Ethiopia, Morocco, South Sudan, Bahamas, Fiji, Mozambique, Sri Lanka, Bangladesh, Ghana, Nicaragua, Syria, Guinea, Nigeria, Trinidad and Tobago, Guinea-Bissau, Niger, Tunisia, Botswana, Guam, North Korea, Turkmenistan, Burkina Faso, Guyana, Oman, Uganda, Burundi Haiti, Pakistan, US Virgin Islands, Cambodia, Iran, Palestine, USA, Central African Republic, Iraq, Panama Venezuela, Congo, Jamaica, Yemen, Congo Democratic Republic, Russian Federation(Crimea only) Zambia, Cuba, Laos, Samoa, Zimbabwe, Dominican Republic, Lebanon, Libya.

SIMPLIFIED DUE DILIGENCE (SDD)

The Company may decide to conduct a simplified due diligence, if the customer does not meet any of these risk criteria. In this case, the customer should provide us the following data set:

a) to verify the identity of an individual who performs management functions in an organization or is a shareholder:

* applicant's full name (as per NID or passport);

*date and place of birth;

*nationality;

*physical address (residential and business);

*contact details (E-mail, phone number);

*ID or passport

*PEP status

*US Citizen status

b) for verification of the identity of a legal entity:

*full business name, including any trading name;

*registered or business address with contact details;

*place of incorporation or registration;

*valid commercial or professional license;

*the identity of the directors, managers, shareholders, signatories or equivalent persons with executive authority in respect of the legal entity;

*ultimate beneficial owners;

*copy of memorandum and articles of association.

In the case of SDD we also:

*reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold (55000 AED/15000 EURO or USD for occasional transactions);

*not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established;

*undertake the periodic review of a business relationships less frequently than usual, including reassess the customer's risk profile every year after establishment of the business relationships.

ENHANCED DUE DILIGENCE (EDD)

The customer's risk level is usually high, when assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of money laundering or terrorist financing is high or considerably higher. The customer's risk level is also high if a risk factor as such calls for this. A high risk does not necessarily mean that the customer is laundering money or financing terrorists.

If the Company feels that the risk level of a customer or a person participating in a

transaction is high, the Company shall apply customer due diligence measures pursuant to the enhanced procedure in order to adequately manage the respective risks. The following are deemed situations increasing risks related to the customer as a person:

*the business relationship based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;

*the customer is a legal person or a legal arrangement, which is engaged in holding personal assets;

*the customer is a cash-intensive business;

*the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;

*the ownership structure of the company appears unusual or excessively complex, given the nature of the company's business.

The following are deemed situations increasing risks related to the product, service, transaction or delivery channel:

*private banking;

*provision of a product or making or mediating of a transaction that might favour anonymity;

*payments received from or sent to third parties;

*new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

When the customer meets one of the risk criteria, the Company must conduct EDD. In this case we should request additional data set:

a) for individuals:

*Selfie with passport or ID;

*Video-call;

*Utility bill;

*Bank statement;

*Source of funds;

*other necessary data.

b) for legal entities:

*Source of entity's funds

*Expected turnover

*Nature of business interest

*Authorized representatives (other than controlling persons) and their legal Capacity

*Other information which may be required for conducting identification and verification of the legal entity.

In case of EDD we also:

*conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

*undertake the periodic review of a business relationships more frequently than usual, including reassess the customer's risk profile every 30-90 days after establishment of the business relationships.

Politically Exposed Persons

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to the Company as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. The Company shall imply EDD to PEPs.

A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official. Individuals entrusted with prominent public functions include:

* Heads of state, heads of government, ministers and deputy or assistant ministers;

* Members of parliaments or of similar legislative bodies;

* Members of supreme courts, of constitutional courts or of other high-level judicial bodies the decisions of which are not subject to further appeal, except in exceptional circumstances;

* Members of courts of auditors or of the boards of central banks;

* Ambassadors, charges affairs and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level);

* Members of the administrative, management or supervisory boards of State-owned enterprises; and

* Directors, deputy directors and members of the board or equivalent function of an international organization.

Family members of PEPs:

* The spouse, or a person considered to be equivalent to a spouse of a PEP;

* The children and their spouses, or persons considered to be equivalent to a spouse, of a PEP; and

* The parents of a PEP.

Persons known to be close associates of PEPs:

* Natural persons, who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP; and

* Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de-facto benefit of a PEP. Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

The following EDD measures in addition to the general CDD measures should be applied to PEPs

* obtains approval from the senior management to establish or continue a business relationship with the person;

* applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship;

* designation of custom transaction limits based on a verified source of funds/wealth;

* monitors the business relationship in an enhanced manner.

TRANSACTION MONITORING

Monitoring and identifying of unusual and suspicious transactions is an important part of customer due diligence measures applied by obliged entities, that allows to identify the circumstances that may point to money laundering or terrorist financing in the activity of customers. Also, the purpose of transaction monitoring is to identify transactions with subjects of international sanctions and politically exposed persons and detect and notify of transactions whose limit or other parameters exceed the prescribed value over a certain period of time.
Transaction monitoring measures can be divided into two categories: screening and analysis.
Transaction screening allows transactions to be monitored in real time, based on data accompanying the transaction. The following “red flags” may be identified upon transaction screening:
* politically exposed persons involved in transactions;
* transactions with persons whose name, alias, date of birth or other identifiable information match with data in lists of persons subject to international sanctions, adverse media, enforcement actions, etc.;
* payments received from or sent to a high-risk country;

* payment received from or sent to a third-party (non-customer of the Company)

Transaction analysis helps to detect deviations in customer's activity and identify unusual transaction patterns which may be related to money laundering, terrorist financing or other illegal activity. The following red flags may be identified upon transaction analysis:

* single large international payments (e.g. whereby the sum ends with at least four zeros);
* accounts with the highest turnover in the period under review based on currencies;
* the largest transactions in the period under review based on different currencies;
* single transaction that exceed the limit, which are made by customers whose turnover is small;
* sudden increase in account activity without rationale;
* transactions in multiple currencies;
* transactions without apparent lawful or business purpose.

If the customer is regularly unable to give the requested information about the nature of transactions or their purpose, the Company shall take measures which include giving warnings and setting time limits. Thereafter the customer may be denied to execute any transaction or business relationships may be limited or terminated.

AML COMPLIANCE OFFICER

The Board shall appoint a compliance officer for performance of AML/CFT duties and obligations. The functions of a compliance officer may be performed by an employee or member of the Board or several employees and/or a business unit with the relevant duties. If the functions of the compliance officer are performed by a business unit, the head of the relevant business unit will be responsible for the performance of the functions.

The position of a compliance officer within the Company shall allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing.

The duties of the compliance officer include:

* Organization of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the Company (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the Company, and analysis of the information contained in them);

* Reporting to the Financial Intelligence Unit (the "FIU") in the event of suspicion of money laundering or terrorist financing (notice being given in the manner agreed with the FIU);

* Periodic submission of written statements on implementation of the rules of procedure to the Board; and

* Performance of other obligations related to the fulfilment of the requirements of the policy (including training employees and applying respective control mechanisms).

The compliance officer shall have access to the information used for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the customer. The management board also grants the compliance officer the right to participate in the meetings of the management board if the compliance officer deems this necessary to perform their functions.

The contact details of the compliance officer shall be communicated to the Financial Intelligence Unit. The compliance officer shall inform the Financial Intelligence Unit within a reasonable term about the appointment of a new compliance officer or a change in contact details.

REPORTING

The compliance officer is advised to make every employee aware of his/her role and duty to receive or submit internal suspicious activity reports.

The compliance officer is advised to investigate suspicious transaction reports (STR) internally and create an internal report outlining the outcome of its investigation including the decision on whether or not to file an external STR. Where appropriate, the compliance officer is advised to make the STR to the FIU and provide a copy to DMCCA.

If a compliance officer suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity, or are related to Money Laundering, Terrorist Financing activity, the compliance officer must file a written STR with the FIU.

To file STR the goAML system should be used: https://services.cbuae.gov.ae/

To file a copy of STR to DMCC: https://dmccpoc.force.com/DMCCHelpCentre/

OUTSOURCING

The Company has the right, considering special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of services by the Company to its Customers [and third party services would be use as addition to the Company standard procedures without relieving the company of responsibility for fulfilling its obligations]. For the purposes of this section, third parties include, for instance, agents, subcontractors and other persons to whom the Company transfers the activities relating to the provision of the services provided as a rule by the Company in its economic activities.

As an example, the Company can use external services,[in addition to its standard procedures], to conduct an Enhanced Due Diligence if there are any suspicious about the customer's data.

RECORD KEEPING

The Company will principally retain the following records from an AML perspective:

* Records of customer screening (PEPs & Sanctions);

* Copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the customer relationship;

* Details of customer transactions for five years from the date of the relevant transaction;

* Records of all AML/CTF training delivered;

* Details of actions taken in respect of internal and external suspicion reports;

* Details of information considered by the MLRO or his nominee in respect of an internal report where no external report is made.

Director/Malkerov Aleksei