DMS Capital AG
Metallstrasse 8, CH-6300 Zug, Switzerland

Anti-Money Laundering Policy

DMS Capital AG

Last update: 2022 July 11

DMS CAPITAL

Table of Contents

DMS CAPITAL

ABBREVIATIONS

AML	Anti-Money Laundering
AMLD5	Anti-Money Laundering Directive 5th
ARIF	Association Romande des Intermédiaires Financiers
CDD	Customer Due Diligence
CTF	Counter-Terrorism Financing
DD	Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FINMA	Swiss Financial Market Supervisory Authority
ID	Identity
KYC	Know Your Customer
ML/TF	Money Laundering/Terrorism Financing
ODD	On-going Due Diligence
ODD	On-going Due Diligence
SAR	Suspicious Activity Report
SO-FIT	Supervisory Body for Financial Intermediaries & Trustees
UBO	Ultimate Beneficial Owner
VA	Virtual Assets

Document changes tracking: 2022-07-11 (date of last changes)

Version:	1st	
Final status:	[Approved]	
1st version legally effective from:	2022-01-01	

Version:	2nd	Updated 2022-07-11
Final status:	[Approved]	
		Signature:
Person who drafted (AML Officer):	Sandra Schaad	Signed 
Person who reviewed (CEO):	Sandra Schaad	Signed 

1. Company information

Company name:	DMS Capital AG
Company number:	CHE-231.535.746
Company address:	Metallstrasse 8 6300 Zug Switzerland
Organization of Supervision:	Swiss Financial Market Supervisory Authority – FINMA
President of the Board of Directors (CEO):	Thierry Jean Pierre Tissot-dit-Sanfin
AML Compliance Officer:	Sandra Schaad
Main email address:	support@dms.capital

2. General introduction

This Anti-Money Laundering (AML) / Counter-Terrorism Financing (CTF) and Know Your Customer (KYC) Policy is designed for DMS Capital AG (hereinafter referred to "DMS Capital AG"), a Swiss Crypto exchange company with company's number CHE-231.535.746, with registered address at Metallstrasse 8, 6300 Zug, Switzerland.

The procedures set forth herein are intended to assist DMS Capital AG in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering, or funding of terrorism, bribery, fraudulent activities, and tax evasion.

DMS Capital AG Compliance personnel and other company's employees using these procedures should also refer, where relevant, to the Act, the Regulations, the

provisions of the Sub-Title, Of Acts of Terrorism, Funding of Terrorism and Ancillary Offences of Title IV A of Part II of Book First of the Criminal Code and any relevant measures/ guidelines which may be issued from time to time by the FINMA and/or any other legally appointed supervisory authority, for instance: Supervisory Body for Financial Intermediaries & Trustees (SO-FIT) and/or Association Romande des Intermédiaires Financiers (ARIF).

When carrying out activities which constitute "relevant activity" DMS Capital AG is required to comply with the requirements of the Prevention of Money Laundering Act, 1994 (Chapter 373 of the laws of Switzerland) (the "Act") and the Regulations which require DMS Capital AG to adhere to the provisions contained in the Act, the Regulations, and the FINMA Implementing Procedures.

This policy is drafted according to Switzerland national Laws:

- Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector. Anti-Money Laundering Act (AMLA);
- The Swiss Financial Market Supervisory Authority on Combating Money Laundering and Terrorist Financing in the Financial Sector. Anti-Money Laundering Act (AMLA).

This Policy is draft according to European Union legislations:

- AMLD5 – Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (5AMLD – 5th EU Anti-Money Laundering Directive);
- GDPR Law – Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Understanding Anti-Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. This is done by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. Generally, money laundering occurs in three stages. In the first step assets enters the financial system at the "placement" stage, where the cash generated from criminal or illegal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy

and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the financial industry is unique in that it can be used to launder funds obtained elsewhere and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, Ponzi schemes, cybercrime, pyramid schemes, advanced fee schemes, foreign currency fraud and other investment-related fraudulent activity.

The Act provides an exhaustive list of acts that constitute money laundering under Swiss Law, as follows:

1) The conversion or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act or acts of participation in criminal activity, for the purpose of or purposes of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity.
2) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.
3) The acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.
4) Retention without the reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity.
5) Attempting any of the matters or activities defined in the above foregoing sub-paragraphs 1), 2), 3) and 4) within the meaning of article 41 of the Criminal Code.
6) Acting as an accomplice within the meaning of article 42 of the Criminal Code in respect of any of the matters or activities defined in the above foregoing sub-paragraphs 1), 2), 3), 4), and 5).

Understanding the Funding of Terrorism

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex. The terrorist financing is defined in the

EU's Third Money Laundering Directive as "The provision or collection of funds, by any means directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part in order to carry out any of the offences that have been defined as terrorism". As the definition underlines, the focus is on the purpose for using the funds and not on the cleaning process of money. In fact, funding to support terrorism may rely on both legitimate sources and criminal activities. Some scholars therefore argue that terrorist financing is reverse money laundering because the process may start with "clean" money; however, the purpose for which the
money is used is illegal. Certainly, the dirty/clean money divide is not soldi, but overlaps given that there are terrorist organizations that receive most of their funds through illegal sources such as drug trafficking, kidnapping, political corruption, smuggling, illegal financial instruments trade, illicit arms trafficking, robbery, bribery and exploitation of human beings.

Cryptocurrencies

Cryptocurrencies are any form of virtual asset stored on an electronic medium that allows a community of Client who accept them as means of payment to execute transactions in such assets without using a legal currency (Fiat currency).

The threat posed by cryptocurrencies results from the inherent anonymity of such transactions, particularly concerning the beneficial owner of the assets, and from the fact that many cryptocurrency transactions are carried out directly without a financial intermediary and they are thus beyond any regulatory agency's control. The threat is reflected both in the criminal exploitation of the design of cryptocurrencies and in investor fraud. However, the use of cryptocurrencies poses a threat also in other crime patterns: terrorist financing, laundering of funds from the sale of illegal services and products, or drug trafficking, especially by criminal organizations. Cryptocurrencies are particularly well suited for money laundering because of their anonymity.

Just like other countries, Switzerland is vulnerable to this danger because it is complicated for both financial intermediaries and prosecution authorities to establish the identity of the beneficial owner of certain assets. In most cases, the technology underlying cryptocurrencies makes it difficult for owner identity to be established. However, when cryptocurrencies are bought or sold for fiat money, the identity of the beneficial owner(s) of the assets involved can be established.

In accordance with Virtual Assets (VA), be known as Cryptocurrencies, DMS Capital AG takes actions to assess, identify, and take effective action to mitigate the Money Laundering/Terrorism Financing (ML/TF) risks associated with providing or engaging in VA business. As VA raises a lot of anonymity, DMS Capital AG designed the Customer Due Diligence (CDD) process to meet both, international and national standards. The CDD process should help the company in assessing the ML/TF risks associated with covered VA activities or business relationships or occasional transactions above the threshold. Initial CDD comprises identifying the customer and, where applicable, the

customer's beneficial owner and verifying the customer's identity on a risk basis and on the base of reliable and independent information, data, or documentation to at least the extent required by the applicable legal or regulatory framework. The CDD process also includes understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations. Taking into the account the higher risk raised by VA business, DMS Capital AG undertakes to collect and assess the additional information on high-risk customers and transactions in order to identify, and avoid engaging in, prohibited activities. Such additional information may include:

- the purpose of transaction or payment;
- details about the nature, end use or end user of the item;
- proof of funds ownership;
- parties to the transaction and the relationship between parties;
- sources of wealth and/or funds;
- the identity and the beneficial ownership of the counterparty.

Such gathered information combined with Due Diligence (DD) process will help the Company to ensure and mitigate risks raised by VA.

The scope of DMS Capital AG's Policy

DMS Capital AG recognizes and identifies ML/TF as threats to DMS Capital AG's, Switzerland's reputation, and the financial services sector on a global scale.

DMS Capital AG is determined and committed to preventing the carrying out of operations that may be related to ML/TF by establishing procedures on internal control, risk assessment, risk management, and compliance. DMS Capital AG shall comply with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offense of money laundering or funding of terrorism through the abuse of its systems and/or services.

This Policy is a guidance and governance document for the behaviour of DMS Capital AG. All senior management, employees and other associated persons who deal with Client or Clients information are required to acknowledge that they have read and are familiarized themselves with this Policy (see Schedule A). It is expected that the controlled, affiliated, and participating companies, define their directions from these guidelines, considering the special needs and the legal aspects to which they are subjected.

Schedule A is an acknowledgement document, which must be signed by each DMS Capital AG company employee and extended to associated persons who are working with DMS Capital AG company's internal systems and who have direct access to the Company's database and personal information.

Our Commitment

DMS Capital AG supports Switzerland's commitment within the Financial Action Task

Force (FATF) to achieve greater harmonization of national regulations to combat money laundering and terrorist financing and is committed to the highest standards of Anti-Money Laundering (AML) compliance. As such, DMS Capital AG has put in place AML procedures to prevent and mitigate possible risks of DMS Capital AG being involved in any kind of illegal activity.

Third-party service providers

DMS Capital AG currently intends to cooperate with the legitimate, good reputation and licensed (if this is needed by third-party's national law) third-party services providers mentioned in this AML Policy. The expansion of the service providers or third-party providers always must be approved by the President of the Board of Directors (CEO) and other Board Members.

3. The Framework of AML Policy

This AML Policy designed and built as a framework to:

- prevent DMS Capital AG from being used by criminal elements for money laundering, financing terrorism activities, tax evasion, fraudulent or scamming activities both intentionally and on national level;
- enable DMS Capital AG to know and understand it's clients, understanding the nature of business activities of each client, to understand business relations with DMS Capital AG. As certain thresholds will be reached to require additional financial or legal background information;
- put in place appropriate controls for detection and reporting (SARs) of suspicious activities in accordance with applicable laws, procedures, and regulatory guidelines;
- equip employees and contractors of DMS Capital AG with the necessary training and measures to deal with matters concerning AML/CTF and KYC procedures and reporting obligations;
- to securely achieve requirements DMS Capital AG documented a detailed Internal Control Framework defining the required procedural steps and control routines. Permanent adherence to this Framework is paramount to secure and compliant operations of DMS Capital AG. The Framework itself is, therefore, an integral part of this guideline and all-time performance, as well as accurate documentation of required controls, are subject to external audit.

Guidelines of DMS Capital AG operational work

DMS Capital AG adheres to the following principles to prevent money laundering and terrorist financing:

- act in good faith;
- keep clean and accurate recording-keeping of the Company's activities and clients;
- fulfill the applicable provisions for the business activity, in particular the Anti-Money Laundering Act and the relevant norms of the Swiss Criminal Code, especially Art. 305-bis, 305-ter, 260-ter and 260-quinquies Swiss Criminal Code;
- inform the Clients about the legal provisions of the AML/CTF and its effect on the business relationship;
- adopt procedures in the development of the DMS Capital AG platform, to inhibit its use for illegal practices linked to money laundering, terrorism financing, tax evasion, corruption;
- do not accept the movement of resources through anonymous checking accounts or linked to fictitious holders;
- use specific parameters for the monitoring of financial transactions that might set up evidence of corruption;
- reject acts of corruption, money laundering, financing of terrorism or any other illegal acts;
- do not on-board or start any business relations with Sanctioned Persons or companies or Shell companies, Shell banks, Government Institutions, Non-profit Organizations, Charities.

Our Duties and Responsibilities

DMS Capital AG, as a licensed Crypto exchange company set these strict duties and main responsibilities to ensure that all clients and all operations are out of grey area, or they are related to any economical criminal activities.

Therefore, these are the main subjects:

- we do not accept, hold, or assist in the investment or transfer of assets which we know or logically assume, are derived from a criminal activity or a qualified from tax evasion, assets acquired from criminal organizations, or are intended to use in purpose of financing terrorism;
- we commit to anti-money laundering according to Art. 305bis SCC, if we take actions which are designed to obstruct the investigation of the origin of the source, the discovery or confiscation of assets which we know, or logically assume, are derived from a crime or a qualified tax offense;
- we must not maintain business relationships with companies or persons whom we know, or logically assume are related to finance terrorism, or support such a

criminal organization in any form. We are liable to prosecution according to Art. 305-ter SCC if, while acting in a professional capacity, we accept, hold, invest, or assist in transferring third-party assets and fail to establish the identity of the beneficial owner with the care required in the circumstances;

- we are liable to prosecution according to Art. 260-quinquies para. 1 SCC, if we intentionally collect, or make available, assets with the intent to finance a violent crime through which the population, a state or an international organization is compelled to act or refrain from acting;
- we adopt procedures of due diligence for mitigating the risks of money laundering, terrorism financing and corruption, according to the activity, jurisdiction and the agents involved;
- we adopt restrictive character measures as for the achievement of business and the maintenance of negotiating relationships with Client's suppliers, and partners when the circumstances reveal evidence of engagement in acts linked to money laundering, terrorism financing or corruption, observed the current legislation;
- we consider, in maintaining a business relationship with partners and suppliers, the existence, within the context of those third parties of mechanisms to prevent corruption;
- we must verify the identity of each customer and representatives of the legal entities;
- we must establish the identity of each Ultimate Beneficial Owner (UBO) of corporate customer;
- we must understand and validate the nature and purpose of the business relationship with each client, both natural and legal person.

4. Compliance procedures

AML Officer – role and relevance

DMS Capital AG has appointed it's AML Officer who is fully responsible for designation and implementation of AML Policy and other Compliance procedures and programs. The AML Officer has as a professional working knowledge of the Compliance programs, AML best practices implemented across the EU and Anti-Money Laundering Act and the relevant norms of the Swiss Criminal Code, especially Art. 305-bis, 305-ter, 260-ter and 260-quinquies Swiss Criminal Code and is qualified by experience, knowledge, and training. DMS Capital AG shall ensure that the AML Officer has sufficient resources available, including appropriate staff and technology, to be able to monitor the day-to-day operations of DMS Capital AG to ensure compliance with its AML Policy. The AML Officer has a direct reporting line to the Board of Directors. The AML Officer has the authority to act independently in carrying out his duties and has full and unlimited

access to the Company's records, data documentation, and information for the purposes of successfully fulfilling his responsibilities. The duties of the AML Officer will include monitoring the firm's compliance with AML/CTF and KYC obligations and overseeing communication and training for employees. The AML Officer will also ensure that the firm keeps and maintains all the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Officer is vested with full responsibility and authority to enforce DMS Capital AG's AML Policy and other AML relevant procedures.

The AML Officer supervises all aspects of AML/CTF, including but not limited to:

a) Collecting and evaluating potential client's identity (ID) information;
b) Establishing and updating internal AML Policy and other relevant procedures for the completion, review, submission, and retention of all reports and records required under the applicable laws and regulations;
c) Monitoring transactions and investigating any significant deviations from normal activity;
d) Implementing a records management system for appropriate storage and retrieval of documents, files, forms;
e) Providing law enforcement with information as required under the applicable laws and regulations;
f) Filing SARs with the FinCEN when appropriate;
g) Interacting with law enforcement involved in the prevention of money laundering, terrorist financing, and other illegal activities;
h) Reporting to DMS Capital AG's the Board of Directors any necessary topic related with Compliance program, change of technological tools, implementation of new tools;
i) Advise company's Board of Directors on a arise questions related to Compliance, AML/CTF sphere or any related topics;
j) Assistance with AML audit when needed.

Customer Due Diligence procedure

In terms of its obligations at law, DMS Capital AG is obliged to determine the applicant for business, the Client, or any beneficial owner, and to verify that such person is the person he purports to be, as well as to determine whether such person is acting on behalf of someone else, and to establish the purpose and intended nature of the business relationship and to monitor this relationship on an ongoing basis. To successfully adhere to its obligations, DMS Capital AG has developed CDD measures which must be implemented to all types of clienteles, both natural and legal clients, and adhered to its management and staff.

The DD measures assist DMS Capital AG in determining whether a particular client falls within their risk appetite, as well as helps the Company clearly understand the business activities of the client in such a way that any transactions which fall outside the business profile of the company may be investigated to determine whether any money laundering or funding of terrorism may be involved. This enables the Company to inform SO-FIT and/or FINMA in a timely manner with adequate information on its client and their activities when such a request is made.

In Summary, DMS Capital AG has adopted its DD procedures to successfully carry out the following:

a) Identification and verification of the applicant for business;
b) Identification and verification of the beneficial owner at all times;
c) Obtaining information on the purpose and intended nature of the business relationship;
d) Conducting ongoing monitoring of the business relationship;
e) Establishing the source of wealth and source of funds for customers when it's necessary;
f) Ensuring that the potential client meets the requirements set out in this AML Policy;
g) Ensuring that all relevant information about UBO must be collected;
h) Ensuring that all relevant information about managing bodies of corporate clients must be collected;
i) Ensuring that all authorized persons, who have or will have any type of access to the corporate client accounts must be identified and verified via appropriate procedure;
j) Conducting ODD (On-going Due Diligence) procedure according to the risk level for each client of the Company;
k) In case of any information changes in client details, ensure that this information is truthful, valid and reflects the current situation about particular client;
l) Continuously monitor transactional patterns and money paths.

Description of potential DMS Capital AG customer

The customers of DMS Capital AG can be:

1) Natural person who is older than 18 years old;
2) Corporate client;
3) Natural person as sole trader or sole proprietor.

Who is Natural person according to DMS Capital AG?

Natural person as a client of DMS Capital AG is 18 years old or more, who is originally lives or resigning not in Prohibited countries list approved by the Company. Natural

person can be a PEP also, with approval of AML Officer and CEO. The company also approves and accepts sole traders and sole proprietors if they do not object to this Policy.

Who is Corporate client according to DMS Capital AG?

Corporate client is described as legal entity, partnership, limited liability company, foundation, non-profit organizations, trusts, or legal entities whose structure contains trusts.

Below is the list of main categories of legal entities which are excepted by DMS Capital AG:

1) Crypto exchange companies;
2) Crypto mining companies;
3) Non-Banking Financial Institutions;
4) Commercial and Specialized Banks;
5) Trading companies;
6) Trusts;
7) Non-profit organizations;
8) Wealth management companies;
9) IT development companies;
10) Any other legal entity whose business is not involved in financial crime or human trafficking or Financial Pyramid (Ponzi schemes), Money Mule schemes, Pump & Dump Scheme, Boiler Room Scheme, drug trafficking or any other form of illegal activities.

This list is not conclusive, as new businesses arise perennially.

DMS Capital AG does not accept Clients with these business areas:

1) Shell banks;
2) Shell companies;
3) Walk-in customers;
4) Illegal immigrants;
5) Persons or companies who are sanctioned;
6) Anonymous clients;
7) Counterfeit products and replicas manufacturing or selling companies or individuals;
8) Any other illegal business activity involved or supporting financial crime or human trafficking or Financial Pyramid (Ponzi schemes), Money Mule schemes, Pump & Dump Scheme, Boiler Room Scheme, drug trafficking or any other form of illegal activities.

DMS Capital AG currently does not accept customers from following countries:

1) Afghanistan
2) Burundi
3) Central African Republic
4) Congo DR
5) Crimea/Sebastopol
6) Cuba
7) Federal Republic of Somalia
8) Gaza Strip
9) Guinea
10) Haiti
11) Iran
12) Iraq
13) Libya
14) Mali
15) Myanmar
16) North Korea
17) Pakistan
18) South Sudan
19) State of Eritrea
20) Sudan
21) Syrian Arab Republic
22) Venezuela
23) Yemen

Customer On-boarding procedure for natural persons

In order to start using DMS Capital AG services, potential customer must perform these steps:

1) Verify his identity via Globalpass identity verification system (or any other approved identity verification system by Board of the Directors);
2) Fill in Natural individual application form;
3) Provide valid and not older than 3 months Proof of address document.

Customers On-boarding procedure for corporate clients

In order to start using DMS Capital AG services, potential customer must perform these steps:

1) Verify authorized person's identity via Globalpass identity verification system or any other equal and qualified system;
2) Fill in Corporate Application form;

3) Provide valid passport or ID card copies of all company's UBOs, Senior management and Representatives;
4) Provide valid and not older than 3 months Proof of address documents for all company's UBOs, Senior management and Representatives;
5) Provide corporate documentation which depends on case-by-case boarding:
    - Provide Certificate of Incorporation document or Extract from National Registry;
    - Provide Articles of Association or Memorandum or Bylaws;
    - Share registry or list of shareholders;
    - Ownership chart when company have two or more ownership layers;
    - Licence copy (when company is licensed entity);
    - AML Policy (when company is dealing in financial services business);
    - Financial statements (applicable when Source of Funds information need to be obtained);
    - Trust agreement/Trust deed (when applicable);
    - Certificate of Good Standing (when applicable);
    - Certificate of Incumbency (when applicable).

The final set of documents may vary depending on business type, model and overall potential customer picture.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) is essentially a process of investigating a higher-risk customer more thoroughly than any others. This process designed to obtain extra information about potential customer and his background and risk that he possesses. DMS Capital AG apply EDD procedure for all high-risk customers whether it is On-boarding or ODD processes. Also, increased DD measures may be applied for customers who do not have high-risk indications.

On-going Due Diligence procedure

The ODD procedure is a process when the Company obtains and renew main information about its customers after some time. It also refers to the ongoing process of ensuring that documents, data, or information collected under the CDD process is kept up to date about all existing customer records. The timeframe for ODD process is depending on the risk level of customers.

All natural persons must go through ODD process in this manner:

- Low risk customer – every 3 years
- Medium risk customer – every 2 years
- High risk customer – once per year

All corporate clients must go through ODD process in this manner:

- Low risk customer – every 3 years
- Medium risk customer – every 2 years
- High risk customer – once per year

Additional client verification step

DMS Capital AG Compliance/Onboarding associate may decide to call the potential client for a short interview before taking final decision to on-board or not on-board the client. The reason of this short interview is to obtain information about client's personal or business accounts needs and reasons to open an account with the Company or to obtain information about specific transaction or set of transaction in certain timeline.

On-going Client activity monitoring and analysis

- Our KYC system uses ongoing automated Client activity monitoring (with automated triggers for investigation) for events such as larger than usual transactions or transaction volume, unusually frequent or large banking or cryptocurrency deposits and withdrawals, deposits from new bank accounts, etc.;
- Our KYC system receives ongoing updates about the details submitted by its client (from GlobalPass). Such as document expiration dates, reports of stolen or reported as lost documents, address changes, new records in section list Interpol, Europol, etc.;

High risk client procedure and guidelines

The potential customer of DMS Capital AG is considered as a High-risk customer, if he fits into one of the below mentioned types:

a. Residence and/or operating address of the Client or UBO is in one of the countries designated as High-risk countries (please see Annex 1);
b. The Client conducts or sends or receives frequent payments to/from one of the countries designated as high-risk countries;
c. A business relationship will be established with domestic and foreign Politically Exposed Person (PEP) or his family member or closed relatives;
d. Business relationship with a PEP in a leading function in an international sports organization or with their family members or close associates;
e. Domicile, residence or place of business activity of the Client or the beneficial owner or their nationality are in a country without effective measures to combating money laundering;
f. If a high risk of ML/TF is identified on the basis of the risk assessment process established by the company;

g. The business relationship, the level of assets or the transaction volume seem under consideration of the Client profile or the circumstances unusual unless its legality is clear.

Specific situations when High-risk is applied for customers:

- Clients whose predominant source of funds is derived from a cash or cash-equivalent transactions, cryptocurrency exchanges, and third-party payment providers;
- Excessive inflows and outflows that do not seem to correspond to the specific Client's known source of funds;
- Legal entities or non-profit organizations transacting by using cryptocurrency exchanges in a way that would be expected of private individuals (could be a sign of a shell company or shelf company);
- Transactions that are structured and micro-structured to evade record-keeping and restrictive thresholds;
- Situations where multiple Clients send similar values in a similar timeframe to DMS Capital AG;
- Fast outgoing cash and cash-intensive activity;
- Rapid flow-through of funds to external financial institutions, where deposit and outflow activity appear similar in aggregate value and timeframe;
- Large purchases of real estate, automobiles, aircrafts and boats.

5. DMS Capital AG identity verification procedure and guidance

DMS Capital AG uses GlobalPass system – (https://globalpass.ch/), a sophisticated fully integrated artificial intelligence identity verification system, which carefully collects and analyses the documents before approving the Clients account.

Standard Client's information collection is performed automatically. Automated information collection includes:

- Identity document submission via webcam (photo);
- Video recording (9-10 sec.) rotating the head of applicant to catch all face features;
- Geolocation details of live verification place;
- Address details collection during live verification.

Standard ID document analysis:

DMS Capital AG through GlobalPass conducts the following automated and manual (combined) processes on passport documents submitted by Clients of DMS Capital AG:

- System scans and analyses the ID document's MRZ code, checking if it matches the MRZ's code standard encryption algorithms and that it is valid. It also extracts and decrypts the MRZ code. The decrypted information is then compared to the information on VIZ of the document. If decrypted information does not match ID document information, the document is marked as suspicious + barcode parsing & crosschecking;
- The photo on the ID document is analyzed and compared to the selfie video. If biometric data does not match it's marked as:
    a) suspicious for using different person's document;
    b) biometrics failed and had to be resubmitted (bad lighting, outdated face picture, etc.).

DMS Capital AG in addition can use other various document analytical tools in order to verify and analyze potential client's submitted documents.

DMS Capital AG screens each potential Client for the following:

1. **Person Search and Initial Analysis**

✓ Advanced Document Analysis

Inspects secure document patterns, examination of sensitive document information, verification of sensitive document information, verification of the address, size and angles and comparison against official databases.

✓ Document Encryption Analysis

Using the MRZ encryption algorithm. If the MRZ code is correct, MRZ is decoded, and the extracted information is matched against the information displayed in the passport. If any data placements, fonts, spacings are incorrect, the document is either:

a) Will not be recognized by the system (and not validate);
b) The system will show errors in data extraction.

Extracted information and security patterns are recorded securely. Identical procedures are used for: passports, ID cards, driver licenses, resident permits (they must be machine-readable documents containing T-1, T-2, T-3 MRZ codes).

GlobalPass checks if passport information matches the country of origin and official document standards.

GlobalPass scans all passports every 24 hours to ensure they have not expired.

✓ Document Biometric Data Scan

Client records a face video via device camera in the Globalpass widget. From the recorded video, the system chooses random snapshots for analysis of distinct facial information, among other information:

a) Detects and measures distances between facial features and what is the percentage match between each snapshot and ID face pic. Shows AI-detected age range, gender;
b) Facial scan results are matched against ID photo. The result is presented as a ratio (in percentages) of video and ID photo match. Results from all biometric scans are securely stored on the database.

✓ Person's Background and History Check

- Adverse media scan against PEP, sanctions list and global lawsuits, bribery, money laundering legal cases;
- In addition, DMS Capital AG Compliance can initiate Google search to obtain more information about potential client. It is performed using search results with a client's name are analyzed against a number of proprietary keywords such as: 'fraud', 'scan', 'lawsuits', 'politics', etc.

✓ AML / PEP / Sanction Screening Categories

- **Adverse Media**: Adverse Media scan looks for published news sources described a crime that was committed. Sources scanned include websites, international newspapers, magazines and periodicals, broadcasts, press releases, and news wires;
- **PEP**: The PEP category contains information about individuals who act in a senior prominent public function, their family members, and associates. The FATF and the Wolfsberg Group broadly outline PEPs as individuals who are or have been entrusted with prominent domestic or foreign public positions. These positions include heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned enterprises, and senior political party officials. The PEP matches are classified as Primary PEP, and Secondary PEP, and grouped in hierarchical order (if a screened person matches two PEP categories, the category from the higher group will show up as the primary finding in the report);
- **Sanctions**: A sanction is a legal and public decree by a regional organization, an international organization, or sovereign government that imposes restrictive measures on a foreign state or entity to advance certain foreign policy or national security objectives.

2. Video authentication

Since the business relationships are entered into over the DMS Capital AG platform, DMS Capital AG verifies that the submitted ID document belongs to the Client via GlobalPass video verification system, which takes a video of the person and analyses it along with the submitted ID document to make sure it's a match. In this way, the document is authenticated. The Client records a live video via device camera.

From the recorded video, the system chooses random snapshots for analysis of distinct facial information, among other information:

- Detects and measures distances between facial features;
- What is the percentage match between each snapshot and ID face picture;
- Shows AI-detected age range, gender;
- Facial scan results are matched against ID photo. The result is presented as a ratio (in percentages) of video and ID photo match.

6. The E-wallet

Monitoring and control of cryptocurrency e-wallets from which Client's receive cryptocurrency funds.
In accordance with FINMA Guidance 02/2019, Payments on the blockchain, 26 August 2019 DMS Capital AG will implement external cryptocurrency wallet monitoring and control system. The DMS Capital AG wallet is a non-custodial wallet.

- Clients are allowed to make cryptocurrency transfers only from their private non-custodial wallets which are assigned to them;
- Blockchain Intel is employed by the operator of the wallet to automatically scrutinize cryptocurrency transactions. Blockchain Intel monitors whether or not the cryptocurrency originated from or passed through a known dark web wallet, wallets associated with stolen bitcoins, major exchange hacks, etc.;
- All transactions regarding cryptocurrency are executed by the Client; neither DMS Capital AG nor our custodian banks have any access to Client wallets or their private keys;
- All crypto liquidity providers that DMS Capital AG working with, have strict VA monitoring rules and tools.

7. Suspicious Activity Report (SAR)

The AML Officer will also ensure that the firm keeps and maintains all of the required AML records and will ensure that SARs are filed with the FinCEN when appropriate.

The anti-money laundering system currently used in Switzerland draws a distinction between SARs based on the intensity of suspicion of money laundering. These suspicions fall into one of two categories: (1) cases where there are reasonable grounds for suspicion, or (2) cases where there is merely a suspicion. Each of these two categories is dealt with by two separate pieces of legislation (Article 9 Anti-Money Laundering Act AMLA or Article 305ter paragraph 2 Swiss Criminal Code SCC), which in turn have different consequences for the financial intermediaries and the authorities.

When confronted with a business relationship where elements justify the submission of a SAR to MROS, the financial intermediary must first determine whether the case falls within the scope of application of Article 9 AMLA (https: www.admin.ch/opc/en/classified-compilation/19970427/index.html#a9) or Article 305ter paragraph 2 SCC. However, the financial intermediary is not free to choose between the application of these two provisions: in the first case, he has a duty to report, whereas in the second case he has a right to report.

The most recent SAR reporting form and accompanying Factsheet can be found here: https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung/meldeformular.html.

8. Trainings

New employees receive AML training as part of the mandatory new-hire training program. All applicable employees are also required to complete AML training annually. We review regularly whether certain employees require specialized additional training. In addition to the below, all employees and other associates shall be required to read and sign-off that they have read and understand this AML Policy in its entirety.

Training should include, at a minimum:

- How to identify red flags and signs of money laundering that arise during the course of the employees' duties;
- What to do once the risk is identified;
- What employees' roles are in our compliance efforts and how to perform them;
- The disciplinary consequences (including civil and criminal penalties) for non-compliance.

All AML Officers are required to take SO-FIT's AML course. All employees and associates

who have access to Client information will be required to complete a CPD certified training course promptly after being hired and yearly. Participation in additional targeted training programs is required for all employees with day-to-day Compliance, AML/CTF related responsibilities. For example:

- Client due diligence measures;
- Record-keeping procedures;
- Internal reporting procedures;
- The recognition and handling of suspicious transactions;
- Procedures on risk assessment and risk management.

DMS CAPITAL

Schedule A

AML Policy acknowledgement of employee

I have read and I understand the DMS Capital AG Anti-Money Laundering Policy and will comply with its procedures to the best of my ability.
I will review this AML Policy regularly and will use it as a reference throughout my time that I'm working at DMS Capital AG. I understand that DMS Capital AG has zero tolerance for violations of this AML Policy and such violations will result in fines and/or termination of employment.

I hereby agree to strictly comply with the DMS Capital AG AML policy

_____ _____

Signature of Associated Person Date

_____

Full name

DMS CAPITAL

ANNEX 1

HIGH-RISK COUNTRIES LIST BY DMS CAPITAL AG

High-Risk Countries
Albania
Algeria
Anguilla
Angola
Antigua and Barbuda
Argentina
Aruba
Azerbaijan
Bahamas
Bangladesh
Barbados
Belarus
Belize
Benin
Bermuda
Bolivia
Bosnia and Herzegovina
Botswana
Brazil
British Virgin Islands
Burkina Faso
Cayman Islands
Cambodia
Cameroon
Cape Verde
Caribbean Netherlands (Bonaire, Sint Eustatius & Saba)
Chad
China
Comoros
Curacao
Cyprus
Djibouti
Dominican Republic
Dominica
Ecuador
Egypt
Equatorial Guinea
Eritrea
Eswatini (Swaziland)
Gabon

Gambia
Ghana
Gibraltar
Guam
Guatemala
Guernsey
Guyana
Guinea-Bissau
Honduras
Hungary
India
Ivory Coast
Jamaica
Jersey
Jordan
Kazakhstan
Kenya
Kyrgyzstan Republic
Kiribati
Kosovo
Laos
Lebanon
Liberia
Macau SAR China
Madagascar
Malawi
Malta
Marshall Islands
Mauritania
Mauritius
Mexico
Moldova
Monaco
Mongolia
Morocco
Mozambique
Nepal
Nicaragua
Niger
Nigeria
Panama
Papua New Guinea
Paraguay
Philippines

Russia
Saint Kitts and Nevis
Samoa
Samoa (American)
Seychelles
Senegal
Serbia
Sierra Leone
South Africa
Sri Lanka
Saint Lucia
Saint Vincent's & Grenadines
Tajikistan
Tanzania
Thailand
Togo
Tonga
Trinidad and Tobago
Tunisia
Turkey
Turkmenistan
Turks and Caicos
Tuvalu
Uganda
Ukraine
United Arab Emirates
United States of America
Uzbekistan
Vanuatu
Vietnam
Zambia
Zimbabwe