

AML POLICY

AML policy means preventing criminals to use services of Interspin s.r.o. (Company identification number 48 038 105, Severovcov 7, 85110, Bratislava, Slovakia) with the aim of money laundering, terrorist financing or other criminal activities.

Money laundering is the process of converting funds, received from illegal activities (such as fraud, corruption, terrorism, etc.), into other funds or investments that look legitimate to hide or distort the real source of funds.

The process of money laundering can be divided into three sequential stages:

- **Placement.** At this stage funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the Company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.
- **Layering.** Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.
- **Integration.** Funds get back into circulation as legitimate to purchase goods and services.

To prevent money laundering, Interspin s.r.o. neither accepts nor pays cash under any circumstances. The Company reserves the right to suspend any client's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

The Company reserves the right to suspend any customer's operation, that can be referred to as illegal or, may be related to money laundering in the opinion of the Company staff.

Company's procedures

Interspin s.r.o. will make sure that it is dealing with a real person or legal entity. Interspin s.r.o. also performs all the required measures in accordance with applicable law and regulations, issued by monetary authorities. The AML policy is being fulfilled within Interspin s.r.o. by means of the following:

- know your customer policy and due diligence
- monitoring of client activity
- record keeping
- payment limitations

Know Your Customer and Customer Due Diligence

Effective Customer Due Diligence measures are essential to the management of money laundering and terrorist financing risk. Customer Due Diligence means identifying the customer and verifying their true identity on the basis of documents, data or information both at the moment of starting a business relationship with customer and on an ongoing basis. The customer identification and verification procedures require, first, the collection of data and, second, attempts to verify that data.

During registration process at Company's site all individual customers provide following identification information:

- Customers' full name
- Customers' email
- Also system fixes IP-addresses of current sessions

Therefore we adopt all the necessary measures to establish and verify the identity of our customers and beneficial owners in cases when Company buys cryptocurrencies from customers and we understand risks of these commodities could be collected in criminal ways.

In cases when Company sells cryptocurrencies to avoid fraud traffic and chargebacks Company requests next details in addition:

- High resolution scanned copy or photo of pages of a passport or any other national ID, indicating family name and name(s), date and place of birth, passport number, issue and expiry dates, country of issue and Client's signature.;
- Photo of customer handling document from list above;

Monitoring of client activity

In addition to gathering information from the clients, Company continues monitoring of activities of every client to identify and prevent any suspicious transactions. A suspicious transaction is known as a transaction that is inconsistent with the client's legitimate business or the usual client's transaction history known from client activity monitoring.

Company has implemented the system of monitoring the named transactions (both automatic and, if needed, manual) to prevent using the Company's services by criminals.

Company constantly checks that its customers and their relevant persons have not been included in international blacklists. Company regularly monitors the lists – supplied by an external provider – containing the names of parties convicted of crimes relevant for AML/CFT purpose

Relations with specific customers

Company applies enhanced measures in cases of increased ML/FT risk, persons who are or have been entrusted with prominent public functions (politically exposed persons or PEPs) and their close associates or parties in respect of which requests for

information have been received in connection with enquiries by the authorities about offences relevant for AML/CFT purposes.

We refuse to execute transactions, which involve in any way parties included in national or international applicable blacklists (e.g. EU regulations or UN resolutions).

Record keeping

Company will keep all suspicious activity reports and any supporting documentation confidential. It will not inform anyone besides UCML or other regulatory authorities approved by UCML about suspicious activity report.

Payment limitations and retention procedures

To avoid suspicious activities there are limitations of amounts and number of transactions set by Company for payments to/from single account via single payment method:

Operation	Per transaction	Per day	Per month
Payout (buy)	\$10 000	5 transactions	\$20 000 total, 20 transactions
Acquire (sell)	\$10 000	5 transactions	\$20 000 total, 20 transactions

Accounts/relations with shell banks and anonymous companies

Company considers any relations with shell banks to be prohibited. "Shell banks" mean banks that have no meaningful mind and management located within the country in which they are incorporated and licensed, and which are unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

It means that Company doesn't establish customer relations or carry out transactions with shell banks. Furthermore Company doesn't entertain relations to trust agencies and companies, trusts, anonymous companies or companies controlled through bearer shares, headquartered in high-risk third countries.

Employees

All Company's employees, managers and directors must be aware of this policy. Employees, managers and directors who are engaged in AML related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML program must be reported in confidence to the Chief Executive Officer.

Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified. Company regularly ensures that employees are trained to identify and report of transactions, which should be reported to government authorities.