BITCASTLE LLC Anti-Money Laundering Policy

Bitcastle LLC (“BITCASTLE”) is committed to the highest standards of compliance against money laundering (AML) and anti-terrorist financing (CTF).

As a financial company is subject to laws and other forms of regulation of anti-money laundering (“AML”), which results in many particular measures, principles and rules that can be seen by applicants for business, clients or partners while dealing with BITCASTLE itself, its subsidiaries, branches, subordinated enterprises or affiliates. To show the importance and willingness to comply with legal requirements and so to help achieve the goals of such, BITCASTLE has adopted within its structure the policies and measures required by the jurisdictions it is operating in.

BITCASTLE focuses on the following.

- Paying a great attention to each client or partner, especially its background, relevant activities and the verification of identity of every applicant for business and all information provided by such
- Continuously monitoring the activity of clients, partners and their transactions and making sure that they correspond to our knowledge of clients
- Creating and safe keeping records on accounts, transactions, communications with clients and partners, gathered information, concerned internal matters and particular procedures
- Evaluating possible risk of money laundering while dealing with clients and transactions and risk rate our clients
- Applying enhanced due diligence in case of dealing with suspicious persons, trustees, politically exposed persons, clients from non-reputable jurisdictions and large deposits over the threshold limit
- Organizing quarterly and annual external trainings for employees, especially for those who deal directly with clients and partners
- Cooperating with responsible Money Laundering Compliance Officer appointed upon employees of BITCASTLE and approved by the regulatory authorities
- Monitoring changes to relevant legislation,sanction list, and International Financial Regulators relevant guidance and adopting new measures, if necessary
- Prohibiting offering any anonymous account or maintaining business relationship with a shellbank
- Suspicious Transaction Reporting to the competent Authority if deemed suspicious by the Money Laundering Compliance accordingly.

To prevent money laundering, BITCASTLE does not accept or pay in cash under any circumstances. The company reserves the right to suspend the operation of any client, which may be considered illegal or, in the opinion of the staff, related to money laundering.

Further, in case it happens that BITCASTLE is in any way operating within a jurisdiction, where AML rules require some additional measures, BITCASTLE makes sure to meet all the additional requirements and to treat relevant matters accordingly.

KYC Policy

BITCASTLE will ensure that all registered users are real or legal persons. BITCASTLE also performs all the necessary measures in accordance with the applicable laws and regulations, issued by the monetary authorities. The AML policy is being met by the following means:
• know your client's policy and due diligence
• monitor customer activity
• Registry maintenance

1. Know Your Customer

   Due to the company's commitment to AML and KYC policies, each company customer must complete a verification procedure. Before BITCASTLE initiates any cooperation with the client, the company ensures that satisfactory evidence is presented or other measures are taken that produce satisfactory proof of the identity of any client or counterparty. The company also applies increased scrutiny to clients, who are residents of other countries, identified by credible sources as countries, who have inadequate AML standards or who may pose a high risk of crime and corruption and beneficial owners who reside in and whose funds are sourced from named countries.

   a) Individual clients

During the registration process, each client provides personal information, specifically: full name; birthdate; country of origin; and full residential address. The following documents may be required to verify personal information: A client submits the following documents (in case the documents are written in non-Latin characters: to avoid delays in the verification process, it is necessary to provide a notarized translation of the document in English) due to KYC requirements and to confirm the indicated information:
• Valid passport (showing the first page of the local or international passport, where the photo and signature are clearly visible); or
• Driving license with photograph; or
• National identity card (showing the front and back);
• Documents proving current permanent address (such as utility bills, bank statements, etc.) containing the customer's full name and place of residence. These documents should not be older than 3 months from the filing date.

   b) Corporate clients

In the event that the applicant company is listed on a recognized or approved stock exchange or when there is independent evidence to show that the applicant is a wholly owned subsidiary or a subsidiary under the control of said company, no further steps will normally be taken to verify the identity. In the event that the company is not listed and none of the main directors or shareholders already has an account with BITCASTLE, the following documentation must be provided:
• Certificate of incorporation or any national equivalent;
• Memorandum and Articles of Association and statutory declaration or any national equivalent;
• Certificate of good standing or other proof of the company's registered address;
• Resolution of the board of directors to open an account and grant authority to those who will operate it;

• Copies of powers of attorney or other authorities granted by the directors in relation to the company;
• Proof of the identity of the directors
• Proof of identity of the final beneficiary (s) and / or the person (s) under whose instructions the signers of the account are empowered to act (in accordance with the rules of individual identity verification described above).

2. Tracking customer activity

In addition to collecting customer information, BITCASTLE continues to monitor the activity of each customer to identify and prevent any suspicious transactions. A suspicious transaction is known as a transaction that is not consistent with the legitimate business of the customer or with the transaction history of the regular customer known by tracking customer activity. BITCASTLE has implemented the named transactions monitoring system (both automatic and, if necessary, manual) to prevent criminals from using the company's services.

3. Keeping records

Records of all transaction data and data obtained for identification purposes, as well as all documents related to money laundering issues (e.g. suspicious activity reporting files, AML account monitoring documentation , etc.) are kept for a minimum

In cases of an attempt to execute transactions that BITCASTLE suspects are related to money laundering or other criminal activity, it will proceed in accordance with applicable law and report the suspicious activity to the regulatory authority.
BITCASTLE reserves the right to suspend the operation of any client, which may be considered illegal or may be related to money laundering in the opinion of the staff.
BITCASTLE has full discretion to temporarily block the suspicious customer's account or terminate a relationship with an existing customer. For more information you can contact us at support@bitcastle.io