ANTI-MONEY LAUNDERING GUIDANCE FOR CRYPTOCURRENCY EXCHANGE BITOTAL

17 June 2017

1. **Introduction**
    1. Bitotal (the "**Company**") carries on the business of operating an online software platform by which users are able to:
        1. buy bitcoin and other cryptocurrencies in return for payment in fiat currency;
        2. sell bitcoin and other cryptocurrencies in return for payment in fiat currency;
        3. buy and sell bitcoin and other cryptocurrencies in return for payment in bitcoin and other cryptocurrencies (the "**Exchange**").
    2. References in this guidance to money laundering should also be interpreted as references to terrorist financing.
2. **Overview**
    1. Complying with the Regulations is an on-going obligation to maintain policies and procedures which are intended to combat money laundering. These policies and procedures should be properly supported by management controls, kept up to date and communicated to staff.
    2. The Company should adopt a risk based approach, varying the measures taken in light of the assessed risk of money laundering.
    3. Key to the prevention of money laundering is:
        1. the identification and reporting of knowledge or suspicions of money laundering;
        2. the identification of customers;
        3. record keeping.
3. **Policies and controls**
    1. Internal Policies and Procedures
        1. The Company should maintain internal policies and procedures for:
            1. customer due diligence;
            2. reporting;
            3. record keeping;
            4. internal management controls;
            5. risk assessment and management;
            6. the monitoring and management of compliance;
            7. the internal communication of such policies and procedures.
        2. The Company's policies and procedures should take a risk based approach.
        3. The Company's policies and procedures must:
            1. ensure that complex or unusually large transactions, or unusual patterns of transactions, are identified and scrutinised;
            2. specify the additional measures that will be taken to prevent the use of products and transactions which favour anonymity.
        4. The senior managers of the Company are responsible for ensuring that the Company's policies and procedures manage the risk of the Exchange being used for financial crime.
    2. Nominated Officer
        1. The Company's policies and procedures must also:
            1. nominate an individual to:
                i. receive disclosures of suspicious activity from the Company's staff;

ii. report suspicious activity to the Serious Organised Crime Agency

2. ensure that staff disclose suspicious activity to the Nominated Officer;
3. ensure that the Nominated Officer considers such disclosures and, if such there reasonable grounds for knowledge or suspicion of money laundering, reports suspicious activity to the Serious Organised Crime Agency.

2. 'Knowledge' means knowledge of money laundering activity based on information which came to a member of staff or the Nominated Officer in the course of the business of the Exchange.
3. 'Suspicion' means an opinion based on information or circumstances but without any certainty or proof.

3. Controls and Communications
    1. The Company must ensure that internal management controls are put into place in order to be aware of potential money laundering.
    2. Internal controls should include:
        1. identification of senior management responsibilities;
        2. regular provision of information to senior management on the risks of money laundering;
        3. relevant staff training on policies and procedures;
        4. documentation of the risk management policies and procedures;
        5. measures to ensure that money laundering is considered as part of the usual operation of the Exchange.
    3. The Company should regularly assess its policies, procedures and management controls to ensure the risks of money laundering continue to be known and managed.

4. **Risk based approach**
    1. A risk based approach is an approach which is a cost effective and proportionate way to manage the risk of money laundering.
    2. In implementing a risk based approach, the Company should consider:
        1. the risk posed by the customer. The following customers should be considered riskier:
            1. new customers making a large one off transaction;
            2. customers which hold a public or governmental position;
            3. customers operating in jurisdictions known to have a high risk of money laundering.
        2. the risk posed by the customer's behaviours. The following behaviours should be considered riskier:
            1. transactions that do not make commercial sense;
            2. refusal to provide satisfactory ID;
            3. a customer appearing to be acting on behalf of another person;
            4. a willingness to bear or risk uncommercial penalties or risks.
    3. The Company should monitor the risk of money laundering by being aware of patterns of business transactions, including:
        1. unusual increases in business from an existing customer;
        2. transactions which are not in keeping with a customer's known activity;
        3. unusual increases of activity at particular times;
        4. unfamiliar or atypical types of customer or transaction.
    4. Risk based control procedures include:
        1. taking customer identification;
        2. verifying customer identification;
        3. taking additional customer identification or implementing enhanced customer due

diligence in the case of higher risk.

5. **Customer due diligence, identification and monitoring**
    1. Customer Due Diligence
        1. The object of customer due diligence is to identify customers and verify their identity.
        2. Customer due diligence should include checking the list of financial sanctions targets listed on the dutch financial institution (AFM) website. The Company should not do business with a person or entity subject of a financial sanctions.
        3. The Company should be able to demonstrate to AFM that its due diligence measures are appropriate in light of the risk of money laundering by the Exchange.
        4. Customer due diligence should be undertaken before the customer's user account is set up.
        5. Because the Exchange enables non face-to-face transactions, the Company should:
            1. obtain additional documentation or information to establish the customer's identity;
            2. apply additional certification methods to verify the customer's identity;
            3. ensure that the first payment from the customer is carried out by bank payment.
        6. The Company should ask customers to state whether or not they hold or have previously held a prominent public government function and ensure that such customers are treated as high risk.
    2. Identification and Verification
        1. Identification can be documentary, electronic or a combination.
        2. A record should be kept of all evidence taken to establish the customer's identity.
        3. Documentation of identity should be supplemented with additional identification such as a recent utility bill or a bank statement which is less than 3 months' old and which shows the customer's name and address.
    3. Ongoing Monitoring
        1. The Company should monitor customer activity on an ongoing basis.
        2. Ongoing monitoring includes:
            1. scrutinising transactions, including the source of funds;
            2. ensuring information about customers is kept up to date
        3. Monitoring may take place as part of a review of previous transactions and can be manual or automated.
        4. Staff should be trained in conducting ongoing monitoring.
6. **Record keeping**
    1. Sufficient records should be kept to demonstrate compliance with the Regulations, including records of:
        1. policies and procedures;
        2. controls and communication;
        3. customer and transaction risk analysis;
        4. customer due diligence, including evidence of customer identity and any supporting documentation;
        5. ongoing monitoring;
        6. transactions and business records, in a form sufficient to compile an audit trail.
    2. Records should be kept for 5 years, beginning on the date the relationship with the customer ends.
7. **General credit/debit card payments**
    1. Withdrawals are possible via same card which has been used to perform deposit.