ECOMMERCE TECHNOLOGIES LTD

AML/CTF CONTROLS AND PROCEDURES

1. Scope

ECOMMERCE TECHNOLOGIES LTD (the “Company”, “We”) adopted the present controls and procedures in compliance with regulatory framework and our ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CTF) POLICY.
This document sets out the procedures which must be followed by the Company’s employees to enable the Company to comply with its legal obligations. Failure by any member of staff to comply with these procedures may lead to disciplinary action.
Our Company shall actively prevent and take measures to guard against being used for money laundering and terrorism financing activities and any other activity that facilitates money laundering or the funding of terrorist or criminal activities.

2. Function of the Money Laundering Reporting Officer (MLRO)

2.1. The Company’s MLRO Sachin Popat coordinates the AML policies and procedures of the Company, and reports to the Director of the Company.

2.2. MLRO arranges the Company’s AML procedures in compliance with all the requirements under the applicable developments and regulations, including the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, the Proceeds of Crime Act 2002, the Terrorism Act 2000, FCA requirements, and our AML/CTF standards. To this end, MLRO reviews AML requirements and ensures the updates and implementation of our AML systems and controls in accordance with the AML policies and procedures for the Company's compliance strategy. Any changes should be monitored and updated as appropriate.

2.3. The MLRO gains a detailed knowledge of the Company’s customer base, products, services, transactions, geographies, business initiatives, processes, strategies and associated controls, conducts detailed reviews of high risk factors and sanctions risk assessment when the Company establishes business relationships with clients, as well as manages all aspects of client on-boarding / KYC processes.

2.4. The MLRO ensures monitoring of relationships and transactions with clients in compliance with the AML procedures of the Company, and activities within the e-money issue and payment service provision under the respective duties. The MLRO analyzes the information obtained from the customer through verification and reveals the operations subject to monitoring and risk level amendment, where necessary.

2.5. MLRO ensures that the risk assessment results are tracked in accordance with internal standards and presents them to the senior management, and based on the MLRO advice they commonly suggest the risk mitigation strategies and other control functions, where such steps are necessary. MLRO continuously supports processes, methodology, internal framework, and the compliance function of the Company, to routinely communicate and report the state of AML Compliance procedures and risks to the senior management.

2.6. The MLRO also ensures that the Company keeps and maintains all of the required AML/CTF records, and arranges client relevant files systematization for record-keeping purposes.

2.7. The MLRO oversees communication with employees and arranges the targeted training.

2.8. Also, the MLRO processes internal SARs and ensures that, when appropriate, SARs are filed with the NCA. Under SAR investigations, the MLRO prepares case files for review (e.g. media search results, copies of statements/checks, Watch Lists reviewing, results from internal system searches, etc.).

3. Risk assessment on an enterprise-wide level:

3.1. Under a risk-based approach we assess the risks that our services may be used for ML/TF and put in place appropriate measures to manage and reduce those risks. An effective risk-based approach identifies the highest risks of ML/TF that the Company faces and puts in place measures to manage these risks.

3.2. The enterprise-wide ML/TF risk assessment enables to better understand the Company's overall vulnerability to ML/TF risks and form the basis for the Company's overall risk-based approach.

3.3. When assessing enterprise-wide ML/TF risks, we take a holistic view of the ML/TF risk factors we have identified that, together, determine the level of ML/TF risk associated with a business relationship or occasional transaction, that can enable us to mitigate and manage the identified and assessed risk. Thus, the Company takes into account and is based on the following:

1) in respect of the Company's customers:
    - the customer's market / segment;
    - volumes and sizes of its customers' transactions, etc.;
    - customers identified as high risk;
2) in respect of the Company customer's countries/ jurisdictions:
    - countries/jurisdictions that the Company is exposed to through our own activities and/or the activities of our customers;
3) in respect of the products/services, transactions and delivery channels:
    - the nature of the services which we offer to the customers, as well as whether the delivery channels are direct, non-face-to-face;
    - the nature, scale, diversity and complexity of the Company's business activities.

3.4. The Company's established internal procedures to prevent the use of our Company's services in ML/TF, and ensure that appropriate procedures and internal controls are in place to account for both changes in regulations and changes in our business, as well as to update them appropriately on a regular basis.

3.5. For this purpose the Company established an internal system of controls to identify and verify all clients to a reasonable level of certainty. We observe the transaction thresholds for the KYC/CDD measures undertaken to prevent anonymity. We identify and scrutinize

transactions which have no apparent economic or legal purpose, or unusual patterns so that each client's assessment enables us to remain within the acceptable enterprise-wide risk level. The assessment takes into account the proportionality with regard to the size and nature of our business, approved by the senior management, as part of the risk management framework and practices.

3.6. Our AML procedures ensure that if new products, new business practices (including new delivery mechanisms) or new technology are adopted by the Company, appropriate measures are taken in preparation for, and during, the adoption of such products, practices or technology to assess and if necessary mitigate any ML/TF risks this new product, practice or technology may cause.

3.7. We carry out ongoing monitoring to receive, systemize, process and retain the appropriate information, arranging internal enquiries to receive and manage the concerns of staff in respect of the risk assessment and record-keeping.

3.8. The AML relevant staff is educated and received targeted training on how to report any suspicious activity and record all AML activities, and when to escalate the reporting to the MLRO and senior management, as appropriate. This procedure is described in the section on suspicious activity reporting. Our internal procedures ensure that anyone in the Company who knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is engaged in ML/TF as a result of information received in the course of the business or otherwise through carrying on that business is required to comply with: (i) Part 3 of the Terrorism Act 2000; or (ii) Part 7 of the Proceeds of Crime Act 2002.

4. Customer Due Diligence

4.1. We established Know-Your-Client (KYC) procedures to ensure that the identities of all new and existing clients are checked and verified to a reasonable level of certainty. This includes all individual clients, all directors and shareholders, all partners of client partnerships, and every board member of the client.

4.2. As we also issue e-money, we carry out monitoring of our business relationship with the users of e-money and of transactions made using the relevant payment instrument enabling us to detect any unusual or suspicious transactions (where applicable).

4.3. DETAILED INFORMATION about our CDD/EDD procedures is provided as a separate document "**Customer Identification Controls**".

5. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, we identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information is collected for each beneficial owner:

(1) the name;

(2) date of birth (for an individual);
(3) an address, which is a residential or business street address (for an individual), or a post office box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
(4) an identification number, which is a National Insurance number and/or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

DETAILED DESCRIPTION on how we identify BOs when onboarding the customer and checking the ownership is provided in the section **Beneficial Ownership Information CDD & Assessment** of our **Customer Identification Controls**.

6. Due Diligence Requirements for Political Senior Officers and Politically Exposed Persons (PEPs).

We identify whether a customer or his / her beneficial owner, or a relative of such a customer, belongs to the category of PEPs.

Our Company does not establish business relationships with PEPs under on-boarding procedures. However, existing clients sometimes become PEPs after they enter a business relationship, so we monitor non-PEP accounts for a change in the PEP status, customer profile or account activity and update customer information. Under the on-boarding procedure we notify our customers about non-cooperation with PEPs.
We use monitoring procedures based on which we ensure obtaining respective information from the customer, as well as from public sources and respective electronic databases for the purpose of ascertaining and verifying Politically Exposed Persons.

DETAILED DESCRIPTION on how we identify PEPs when onboarding the customer and checking whether he/she is a PEP or not is provided in the section **Due Diligence Requirements and Screening for Politically Exposed Persons (PEPs)** of our **Customer Identification Controls**.

7. Correspondent Relationship

The Company cooperates with other financial institutions and this is associated with higher risks. Therefore, in such cases we must apply enhanced customer due diligence measures and enhanced ongoing monitoring.
Alongside, the Company does not enter into, or continue, any relationship with any shell bank, as well as take appropriate enhanced measures to ensure that the Company does not enter into, or continue, such correspondent relationship with a financial institution which is known to allow its accounts to be used by a shell bank.

EDD for correspondent relationships is provided in the section **EDD obligation for correspondent relationships** of the **Customer Identification Controls.**

8. Understanding the Nature and Purpose of Customer Relationships

7.1. Our approach to establishing a business relationship includes the risk assessment carried out under regulation 18(1) of the MLRs 2017 (the customer, the country, the product/service, the transaction, the delivery channel) and assessment of the level of risk arising in any particular case, by which reason the risk level may differ from case to case.

7.2. In assessing the risk level in a particular case, we take account of factors including, among other things:

(a) the purpose of an account, transaction or business relationship;
(b) the level of assets to be deposited by a customer or the size of the transactions undertaken by the customer;
(c) the regularity and duration of our relationships.

7.3. We take measures to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, which depending on the facts and circumstances, may include such information as:

- The type of customer;
- The account or service being offered;
- The customer's income;
- The customer's net worth;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

7.4. DETAILED DESCRIPTION of our Customer due diligence measures, Additional customer due diligence measures/ Enhanced customer due diligence measures are provided in our **Customer Identification Controls**.

8. Company's Obligation to report discrepancies in registers

8.1. We must obtain proof of registration or an excerpt from the register from the corporate customer, before establishing a business relationship with such customer. If we find any discrepancy between information relating to the beneficial ownership of such customer, we must report this to the registrar (Companies House).

8.2. This concerns a discrepancy between the information that we hold in our records about a beneficial owner of a client's company, limited liability partnership, or Scottish limited or qualifying partnership and the information that's on the public people with significant control (PSC) register. To comply with this requirement, our AML relative employee checks the formed KYC customer profile and compares it with the data from the register. We also notify our customers to inform us on changes in their profile within 14 days (it is indicated in the KYC form of the customer).

9. Company's Obligation to cease transactions

If we are unable to apply CDD measures as required by the MLRs 2017, we:

(a) must not carry out any transaction through an account with the customer or on behalf of the customer;

(b) must not establish a business relationship with the customer;
(c) must terminate any existing business relationship with the customer;
(d) must consider whether we are required to make a disclosure (or to make further disclosure) by: (i) Part 3 of the Terrorism Act 2000; or (ii) Part 7 of the Proceeds of Crime Act 2002.

10. Sanctions Lists

10.1. A sanctions search is part of our Knowing Your Customer requirements.
Sanctions regimes impose restrictions on our ability to do business with those persons and entities which are on sanctions lists (HMT, PEP, UN, EU, OFAC).
The EU and HMT's Office of Financial Sanctions Implementation (OFSI) apply to companies in the UK. OFAC list applies to the business relationships with the US companies or to transactions carried out in the US Dollars.

10.2. The company checks all transactions to confirm that no transaction involves any individual or company on the Consolidated Sanctions Lists. Analysis of sanctions risk is an integral part of the CDD/EDD/KYC requirements.

10.3. There is a separate but related sanctions regime that imposes restrictions on our ability to do business with those persons and entities on sanctions lists. Some entries on the list are specific to a particular person or entity and others are general financial sanctions on all persons and entities in a particular jurisdiction.

10.4. Before opening an account, and on an ongoing basis, our relevant onboarding employee checks to ensure that a customer does not appear on any sanctions list or is not engaging in transactions that are prohibited by the economic or financial sanctions and embargoes administered and enforced by the competent authorities.
Our staff also reviews existing accounts against the persons under sanctions and listings of current sanctions and embargoes when they are updated and, where applicable, they are instructed to document the review including the customer accounts and transactions.

10.5. If we determine that a customer is on the sanction(s) list or is engaging in transactions that are prohibited by the economic or financial sanctions and embargoes administered and enforced by the competent authorities, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with NCA without delay within the reasonable timeframe.

10.6. If there is any potential match with any sanction’s lists (HMT, UN, EU, OFAC, PEP), a trigger activates for the name of the person. Where there is any Sanctions list match alert, MLRO does further checks on that transaction and advice actions accordingly. All alerts on transactions must be stored in our files.

10.7. The Company uses the sanctions and high-risk jurisdictions lists for check-up procedures (including PEP screening) through https://dilisense.com/en_US, which includes multiple consolidated lists.

Additionally, we carry out control double-checks throughout the following lists:

1) Financial sanctions targets: list of all asset freeze targets (including Designated Persons): https://ofsistorage.blob.core.windows.net/publishlive/ConList.html; https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets;
2) Countries that have organisations operating within their territory which have been designated: by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000, as well as other countries with terrorist organisations;
3) High-Risk Third Country with strategic deficiencies (REGULATION (EU) 2016/1675);
4) EU list of non-cooperative jurisdictions for tax purposes
5) FATF list of Jurisdictions with strategic deficiencies (graylist) and high-risk (blacklist);
6) EU sanctions map;
7) UN consolidated list
8) OFAC sanctions list search

Also, we take account of:

9) CPI countries, Basel AML index.

11. Risk Factors.

11.1. Risk factors that signal possible ML/TF include, but are not limited to:

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.
- Customer with no discernable reason for using the company's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with the company's compliance with government reporting requirements and company's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.

- Many small, incoming wire transfers or deposits through money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Transactions Involving Securities

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
- Two or more accounts trade an illiquid stock suddenly and simultaneously.
- Customer journals securities between unrelated accounts for no apparent business reason.
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
- Customer's trading patterns suggest that he or she may have inside information.

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.
- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.
- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- Purchases an insurance product with no concern for investment objective or performance.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of transactions.
- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.
- Law enforcement subpoenas.
- Large numbers of transactions across a number of jurisdictions.
- Money transfers in and out with no purpose or in unusual circumstances.
- Payment by third-party involvement or money transfer without an apparent connection to the customer.
- Payments to third-party without apparent connection to the customer.

- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).
- There are relevant transactions between parties based in high-risk third countries.
- The customer is a third-country national seeking residence rights or citizenship in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities.
- Non-face to face business relationships or transactions without certain safeguards concerning electronic identification processes.
- Transactions related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or archaeological, historical, cultural and religious significance, or of rare scientific value (we do not cooperate with clients for such transactions).

11.2. Responding to Risk Factors and Suspicious Activity

11.2.1. When an employee of the Company detects any risk factor, or other activity that may be suspicious, he/she is instructed to make an internal report (as provided in the section Suspicious Activity Reporting of this document) to notify the MLRO, as appropriate.

11.2.2. Guided by the MLRO, we shall determine whether or not and how to investigate the matter further. This may include gathering additional information internally or from third-party sources, contacting the authorities, freezing the account or, depending on the circumstances, filing an external SAR (with the NCA / competent authorities, as provided below in the Suspicious Activity Reporting section).

12. Ongoing Monitoring and Risk Assessment

12.1. We conduct ongoing monitoring of business relationships with customers, to ensure that the documents, data or information held evidencing the customer's identity are kept up to date. During these procedures we review clients records and compare them with the clients' financial activity to ensure compliance between these data.

12.2. Ongoing monitoring is provided on a risk-sensitive basis, and includes:

(a) scrutiny, tracking and records of *transactions* undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the Company's knowledge of the customer, the customer's business and risk profile;

(b) in respect of e-money, upon e-money issue, we carry out sufficient monitoring of our business relationship with the users of e-money and of transactions to enable it to detect any unusual or suspicious transactions (where applicable)

(c) undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD measures up-to-date, and thus updating periodically existing identification data and ensuring their conformity with current applicable requirements;

(d) maintaining current information and records relating to the client and its beneficial owner.

12.3. Within this procedure we check the clients and their transactions, particularly as following:

- Clients with businesses that handle large amounts of cash (e.g., if an occasional transaction amounts or is just below the threshold, whether the transaction is executed in a single operation or in several operations which appear to be linked) or complex unusually large transactions.
- Clients with larger one-off transactions, or a number of transactions carried out by the same customer within a short space of time (e.g., if an occasional transaction is just below the threshold of 1,000 euros for due diligence checks).
- Clients with complex business ownership structures with the potential to conceal beneficial owners or persons with significant control (PSC).
- Clients based in or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organised crime or drug production/distribution.
- Situations where the source of funds cannot be easily verified.
- Unusual patterns of transactions that have no apparent economic or visible legal purpose.
- Money sent to or received from areas known to have high levels of criminality, AML deficiency or terrorist activity.

12.4. As part of ongoing monitoring, we also conduct event-driven reviews and request an update of the information obtained during the client's onboarding, to assess whether there is any change in the following:

- a change in the client's identity (e.g., a change of the physical person previously identified and verified, or a change of ID/passport of the physical person previously identified and verified);
- a change of the beneficial owner (both for KYC purposes and reporting discrepancies to the registrar);
- a significant change to key office holders;
- a change in the service provided to the client (e.g., a different transaction);
- information that is inconsistent with our knowledge of the client;
- uncharacteristic transactions which are not in keeping with the customer's known activities;
- a significant change in the client's activities, a sudden increase in his/her business or peaks of activity at particular locations or at particular times;
- unfamiliar or untypical types of customer or transaction.
- previously stalled engagement restarting;
- and if we doubt in the veracity of the information provided by the client, or other suspicion.

12.5. Whenever there is cause for suspicion, the client will be asked to identify and verify the source or destination of the transactions, additional information and provide applicable supporting documents.
Other forms of identity confirmation, such as evidence of a long standing relationship with the client, or a letter of assurance from independent and reliable persons or organisations, who have dealt with the client for some time, may also provide a reasonable level of certainty.

12.6. Ongoing monitoring for the financial institution or any customer of regulated sector must

be enhanced, the Company checks:

1. the regulator's register, to have the financial institution or any other customer from the regulated sector registration record up-to-date;
2. the organizational/ownership structure, the senior management, MLRO, BOs, shareholders data;
3. the up-to-date AML/CTF policies in compliance with the applicable regulations, including procedures, risk assessments, sanctions policy, PEPs screening, SARs, transactions monitoring, training, anonymous accounts and shell bank policies, monitoring procedures, and any other data applicable to the customer from the regulated sector (license operator);
4. take additional measures to understand the background and ownership structure, where there is such necessity and reasonable grounds;
5. increase the monitoring of the business/correspondent relationship, including greater scrutiny of transactions where additional measures are necessary.

12.7. The frequency of monitoring reviews in accordance with the risk assessment of our customers is as follows below (or more frequently if the respective circumstances arise) :
- for high-risk customers: every 3 months;
- for medium-risk customers: every 6 months;
- for low-risk customers: every 12 months.

12.8. Pursuant to the section "Company's Obligation to report discrepancies in registers" of this document, in case if we find the discrepancy during checkup of the documentary evidence for a legal entity, we shall report it to the registrar.

12.9. Based on these reviews, the MLRO is required to fill the form "**Ongoing Monitoring of the Client's Profile**", reflect all results, and where necessary to assess the Risk level approval or change.

13. Suspicious Activity Reporting

13.1. Internal and External Reporting.

The key elements for a SAR are: suspicion, crime, proceeds. Where we suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to ML/TF, we must promptly report our suspicions.

Our relevant employees are instructed to file SARs for any transactions, including money transfers and deposits, conducted or attempted by, at or through our Company, where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade the law or regulation or to avoid any transaction reporting requirement under the law or regulation;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the applicable regulations;

(3) the transaction has no business purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction.

Completed SARs must be collected and maintained with any supporting documentation, for record-keeping purposes. All SAR related information and involved transactions must be treated as strictly confidential, except as permitted under the reporting regulations.

13.2. Internal Reporting.

Pursuant to the applicable requirements, our AML relevant team is instructed to fill in the form "**Internal Suspicious Activity Report to the MLRO**" SAR for any suspicious activity or transactions, including money transfers and deposits, conducted or attempted by, at or through our Company, where we know, suspect or have reasonable grounds to suspect:

1. transaction discrepancies;
2. overpaid invoices operations (e.g., the client intends to dishonestly retain the overpayments),
3. invoices lacking commercial rationale (e.g., the transaction involves the payment to the consultancy firm as an intermediary with no confirmed reasons);
4. blacklisted or changed IP address(es);
5. funds shifting to tax havens;
6. the client's unusual cross-border activities;
7. the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade applicable law or regulation or to avoid any transaction reporting requirement under law or regulation;
8. the transaction is designed, whether through structuring or otherwise, to evade any requirements of the applicable regulations;
9. the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction;
10. the funds are flowing to high-risk or blacklisted countries;
11. transactions with missing documents which are additionally required by our employees for check-up and screening, or there are inconsistent explanations;
12. the transaction involves the use of the Company to facilitate criminal activity; or
13. the appropriate law enforcement authority in situations involving violations require immediate attention, such as ML / TF schemes.

Our related employees are educated to file the form "**Internal Suspicious Activity Report to the MLRO**", which must be submitted to the MLRO.

13.3. External Reporting.

If/when our MLRO receives disclosures, he has a duty to consider all internal reported concerns. A review must be initiated promptly upon identification of unusual activity that

warrants investigation, taking into account also all relevant information and supporting documentation from internal, or third-party sources if any, before a SAR is filed.

The MLRO is responsible for deciding whether or not the suspicion of illegal activity is great enough to justify the submission of a SAR. As soon as the MLRO considers that there are criminal proceeds and existing facts constitute a basis for SAR filing, he must file it through SAR Online system in accordance with the requirements set by the UK FIU https://www.nationalcrimeagency.gov.uk.

13.4. 'Failure to disclose'.

If the MLRO fails to file a SAR as appropriate, he may commit a 'failure to disclose' offence under the POCA section 331.

13.5. 'Tipping off'.

The POCA section 333A on tipping off for the regulated sector provides offences of failing to make a SAR and tipping off any person that has made or had an intention to make such a report. It is a criminal offence for anyone to say or do anything that may prejudice an investigation or 'tip off' another person that a suspicion has been raised, a SAR has been submitted or that a ML/TF investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

Also, It is prohibited to inform the customer linked to the reported transaction, if such transaction is delayed because of a suspicion or is subject to the reporting to the NCA, or if law enforcement agencies are investigating the customer.

14. Record-Keeping

14.1. We must keep the following records:

- any documents and information obtained by us for KYC/CDD purposes;
- supporting records in respect of an occasional or not occasional transaction, which relates to the KYC/CDD measures or ongoing monitoring, for the purposes of such transaction reconstruction.

14.2. The records must be kept for a 5-year period beginning on the date when:

- the transaction is complete (for records relating to an occasional transaction);
- the business relationship with the customer is terminated (for records relating to KYC/CDD measures or any transaction in respect of that customer).

14.3. Once the 5-year, or 10-year where applicable, period has expired, the Company must delete any relevant personal data:

- where the Company is not required to retain personal data records under any enactment or court proceedings;
- where the Company does not have reasonable grounds that the personal data are necessary for any legal proceedings;
- if the data subject did not give consent for further retention of his/her personal data.

14.4. All records shall be duly handled, securely stored, and capable of being retrieved without undue delay, when necessary.

15. Training Program

15.1. The Company takes measures to ensure that its AML relevant employees are educated of ML/TF regulatory requirements under MLRs and how to recognise and deal with transactions and other activities that may be related to ML/TF. All AML relevant employees are trained on their responsibilities in relation to ML legislation, and are aware of how to identify and deal with transactions that may involve ML.

15.2. Training takes into account the nature and extent of ML/TF risks to which the Company is subject, as well as the nature and size of business.

15.3. We developed ongoing employee training under the leadership of the MLRO and Senior Management. Our training shall occur on at least an annual basis and is updated as necessary to reflect any new developments in law or our internal policies and procedures.

15.4. We can develop training in our company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos.

15.5. We maintain records to show the persons trained, the dates of training and the subject matter of their training.

15.6. We review our operations to see if certain employees, such as those in compliance, require specialized additional training. Our written procedures are updated to reflect any such changes.

15.7. Our Training Program covers the following:
[Relevant employees are trained to assess and provide the issues following below and the MLRO checks and fills in a report in that regard]

1) Regulatory framework;
- Legislature;
- FCA guides/requirements;

2) Systems & Controls:
- AML/CTF policy and procedural documents review and updating;
- assessment of adequacy to meet the Company’s needs & financial crime risks mitigation;
- effectiveness in meeting the regulatory & legal rules & requirements;
- assessment of existing controls and measures to ensure that the Company can identify, assess, monitor and manage ML/TF risks;

3) Procedures:
- KYC/CDD checks review;
- Ongoing monitoring;
- How to recognise and deal with transactions and other activities that may be related to ML/TF;

- How to identify risk factors and signs of ML/TF that arise during the course of the employees' duties;
- What to do once the risk is identified, including how, when and to whom to escalate unusual customer activity or other risk factors for analysis and, where appropriate, SAR filing;

4) Assessments in respect of:

- whether all training materials are reviewed for compliance with applicable laws and regulations;
- employee's feedback on the training content;
- periodicity of the staff training (e.g., every 6 months);
- last content update/review for training materials;

5) Quality checks performed for awareness and training with regards to ML/TF.

16. Program to Independently Test AML Program

16.1. Staffing

The testing of our AML program shall be performed at least annually on a calendar year basis. Where an independent third party is involved for training, we shall evaluate the qualifications of such independent third party to ensure they have a working knowledge of applicable requirements. Independent testing shall be performed more frequently if circumstances warrant.

16.2. Evaluation and Reporting

After we have completed the independent testing, staff shall report its findings to the senior management, or to an internal audit committee, whichever applicable. We shall promptly address each of the resulting recommendations and keep a record of how each noted deficiency, if any, was resolved.

17. Monitoring Employee Conduct and Accounts

We subject employee accounts to the same AML procedures as customer accounts, under the supervision of the MLRO. We also review the AML performance of supervisors, as part of their annual performance review. The MLRO's accounts can be reviewed by a Director of the Company, or a designated member of senior management, whichever applicable.

18. Confidential Reporting of AML Non-Compliance

Employees can promptly report any potential violations of the Company's AML/CTF policy to the MLRO, unless the violations implicate the MLRO, in which case the employee shall report to the Director of the Company / senior management of the Company. Such reports must be confidential.

19. Approval

Director and MLRO of the Company has approved this document in writing as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of the applicable law and the implementing regulations under it. This approval is indicated by signatures below, with the last updated version on 22.01.2021.

ECOMMERCE TECHNOLOGIES LTD

SIGNED:  **/Serhii Zakharov/**

SIGNED:  **/Sachin Popat/**

Title: Director

Title: MLRO

Date: 22.01.2021