ILEX EXCHANGE LTD KYC and AML Policy

1. Introduction

ILEX EXCHANGE LTD (hereafter ILEXEXCHANGE) is committed to the highest standards of Anti-Money Laundering (AML)
compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes. ILEXEXCHANGE's Know Your Client (KYC) is at the heart of anti-money laundering measure adopted by the company. It is becoming increasingly important globally to prevent identity theft fraud, money laundering and terrorist financing. The company strictly follows all the due diligence policies and procedures of United Kingdom and regulations to identify the principle before the transaction actually takes place.

2. Objectives

The standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements and apply for the entire ILEX EXCHANGE LTD. There requirements are intend to prevent ILEXEXCHANGE, our employees and clients from being misused for money laundering, terrorist financing or other financial crime. This Policy establishes the general framework for the fight against money laundering and financing of terrorism.

3. Roles & Responsibilities under its anti-money laundering policy

ILEXEXCHANGE management is required to establish anti-money laundering policies, procedures and controls. They must train their staff to ensure that such policies and procedures are followed. In order to assist law enforcement, records must be kept of the due diligence performed when opening accounts as well as records of all transactions. Finally, they must ensure that the effectiveness of the anti-money laundering program is independently tested.

Each of the ILEXEXCHANGE operations has made the following officers responsible for its anti-money laundering program:

- Board of Directors
- Chairman of the Board
- Chief Executive Officer
- Compliance committee – Cards and Payments
- AML OFFICER - Controller and Compliance

Boards of Directors

The Board of Directors of each at ILEXEXCHANGE is responsible for the overall conduct and performance of the company. Consequently, the board of directors must:

- Review and approve this anti-money laundering policy and requirements.
- Appoint the relevant officers to implement the policy and procedures.
- Periodically assess the effectiveness of the policy and procedures.

Chairman of the Board

The Chairman is responsible for governance processes at ILEXEXCHANGE. In this context, the Chairman is responsible for:

- Managing the Board of Directors process, including ensuring that their responsibilities are carried out;
- Overseeing external relations with regulators, including anti-money laundering authorities or financial intelligence units; and
- Ensuring that the AML officer - Controller and Compliance, the Risk Management Group and Internal Audit fuiLexExchangeill their obligations under this policy.

Chief Executive Officer

Chief Executive Officer are responsible for the management of ILEXEXCHANGE, and are ultimately responsible for its
performance, including the management of risk and internal controls.

The CEO must ensure that through the Compliance committee - Cards and Payments and the AML OFFICER–

Controller and Compliance:

- There is communication of policy and procedures;
- Sufficient resources are put into anti-money laundering training;
- Client acceptance standards are followed;
- Business transaction records, including declaration of source of funds reports are kept; and
- Unusual Transaction Reports are made to the relevant money laundering reporting officer.

This responsibility includes ensuring that there is management action plans to deal with identified control deficiencies at a bank wide level and that such plans are executed.

Compliance committee– *Cards and Payments*

Compliance committee– Cards and Payments is responsible for e-wallet, credit and debit card business lines and is ultimately responsible for its performance, including the management of risk and internal controls. Compliance committee must ensure, through his staff and business partners (including third parties who have entered into co branding or affinity marketing programs with ILEXEXCHANGE)

- There is communication of policy and procedures;
- Sufficient resources are put into anti-money laundering training;
- Client acceptance standards are followed;
- Business transaction records, including declaration of source of funds reports are kept; and
- Unusual Transaction Reports are made to the AML OFFICER - Controller and Compliance

Ensure that all business Partners, when contracted as such, have put in place policies and processes which ensure the Customer Identification processes required by ILEXEXCHANGE are in place and enforced,

With the support of the AML OFFICER – Controller and Compliance, perform regular audits of Business Partner records to ensure compliance with ILEXEXCHANGE Anti Money Laundering and Know Your Customer Policies

AML OFFICER *Accounting & Compliance*

- Prepare and update Anti-Money Laundering Policy;
- Advise Operations on Anti-Money Laundering Procedures;
- Provide advice to the line on regulatory requirements and interpretation of policy;
- Provide advice to management on risk profile of business, and areas requiring greater scrutiny;
- Assist Management in the execution of anti-money laundering training programs;
- Be responsible for reporting suspicious transactions and dealing with Financial Intelligence Units;
- Assist Management in developing electronic monitoring tools to better monitor large cash transactions, wire transfers and identify other unusual transaction
- reports – until these are transitioned elsewhere, compliance is running these reports; and
- Have financial reporting responsibility for all lines of businesses, for the Bank
- Review and document Unusual Activity Reports, conduct monitoring of Accounts and complete Suspicious Transaction Reports as necessary
- Reporting any requests for information or co-operations from law enforcement to senior management
- Review reports or journals for bank cheques/drafts, wires and similar instruments for amounts over Threshold limits in place (initially US$100,000) and any other

Know Your Client" versus "Client Acceptance Rules"

ILEXEXCHANGE policy is to "know its clients". ILEXEXCHANGE's business is conducted on mainly with Asian countries and the European Union. Client acceptance is just the beginning of the "know your client" which must continue over the whole life of the relationship with that client.

ILEXEXCHANGE's Customer Identification Program is designed to provide the staff with account opening and customer identification guidelines and a general guide to good practices based on the principles of the Basel Committee's *Customer Due Diligence for Banks* paper.

4. Know Your Customer Standards

ILEXEXCHANGE's KYC is a set of guidelines designed for proper identification of an account holder/customer for scrutiny/monitoring of large value cash transaction. It is implemented to make sure that ILEXEXCHANGE knows

the identity of the applicant's correct name, address, company address, and other identical information to determine the individual or corporation at the moment that ILEXEXCHANGE provides with its service to such applicants. Under this policy, in case that any incident which ILEXEXCHANGE may consider as a fraud occurs, ILEXEXCHANGE shall make best effort to prevent further fraud, disclose the information to clarify where responsibility lies.

4.1 Customer Identification Program (CIP)

ILEX EXCHANGE LTD Customer Identification Program is designed to provide the staff with account opening and customer identification guidelines and a general guide to good practices.

4.1.1 Individual Customers/Natural Persons

The following information will be collected prior to the opening of accounts for customers.

- Legal Name
- Permanent Residential Address. This must be a physical address. Post Office Boxes are not allowed.
- Date of Birth
- Identification Number. ID number must be obtained from a valid government-issued identification containing a photograph.
- Telephone Number
- E-mail address

A color copy of Passport or Driver's License (valid for at least 3 months) that is government issued. The ID shall contain customer's legal name, face picture, and Date of Birth, ID number clearly.

- The Copy of the ID needs to be a color copy of the page that contains customer's face picture.
- The whole page with the face picture shall be contained without any lack of the boarder and any letters contained in the ID shall be clear enough to read.
- The copy needs to be the same size as the original document.

ILEXEXCHANGE should verify this information by at least one of the following methods:

- confirming the date of birth from an official document (e.g. passport, identity card, driver's license, social security records);
- confirming the permanent address (e.g. utility bill, tax assessment, bank statement, letter from a public authority);
- contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);
- Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public, bank official).

4.1.2 Corporate Entities/Corporations

For corporations, the principal guidance is to look behind the institution to identify those who have control over the business and the company's partnership's assets, including those who have ultimate control. For corporations, particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals, including any relationships with politically exposed persons. What constitutes control for this purpose will depend on the nature of a company, and may rest in those who are mandated to manage funds, accounts or investments without requiring further authorization, and who would be in a position to override internal procedures and control mechanisms.

Where a company is a private corporation, the key requirement is to verify:

- That the corporation is validly incorporated and existing;
- The beneficial owners of the company;
- The officers and directors of the company; and
- The identity and authority of the individuals representing the company to open and operate the account.

a) Corporate Identity and Existence is proved by one or more of the following:

- A copy of the Company's Certificate of Incorporation;
- Certificate of Good Standing if company is more than 12 months old;
- Location/address of Registered Office or Registered Agent (usually obtained from corporate documents or the Registrar of Companies);
- Operation/Trading Address (if different from the Registered Office);
- Copy of Articles of Incorporation or Memorandum and Articles of Association;
- Mail, Phone, Fax and E-mail address (if any);

b) Nature of the Business and Source of Funds is proved by one or more of the following:

- Description of nature of business, including products or services provided, countries and locations which the company does business;
- Date of commencement of business;
- Copy of license if company conducts licensed business e.g. insurance, bank, mutual fund etc.; and such other official documents and other information as are reasonably capable of establishing the structural information of the corporate entity, business plans, brochures, etc.

c) Beneficial Ownership is proven by one or more of the following:

- Certificate from Corporate Secretary outlining the names and the addresses of all shareholders;
- Letter from Lawyer to Company outlining names and addresses of all shareholders;
- Notes to Audited Financial Statements or letter from Accounting firm;
- Copy of the shareholder's register; or
- Search of corporate records in those jurisdictions where beneficial ownership must be filed with the Registrar of Companies.

If for any reason, it appears that the corporation is being run by nominee directors, who have either no or marginal ownership of the firm, and the company is closely held by one or a few shareholders, it may be advisable to obtain personal identification of those shareholders.
In the case of larger commercial entities, with professional management and directors, who are in fact managing the company, such further due diligence on shareholders may not be necessary.
However, in the case of small business corporations or personal investment entities, where the controlling shareholder(s) are not directors, and there is no identification on record, then personal identification should be obtained.

d) Officers and Directors are proved by one or more of the following:

- Certificate from Corporate Secretary giving names and addresses of officers and directors;
- Search of corporate records in those jurisdictions where directors and officers must be filed with the Registrar of Companies;
- Letter from Lawyer to Company; or
- Notes to Financial Statements or letter from accounting firm.

e) Identity and authority of the individuals representing the company to open and operate the account is verified by the following:

- Banking resolution
- Personal Identification of the signatories to the account and directors that hold more than 25% of the equity of the firm.

Where these individuals are already clients of ILEXEXCHANGE their personal identification of the directors can be cross- referenced to personal account files, rather than obtaining new documents.

f) As part of the account opening procedure, we should understand and document the expected turnover and source of the funds for the account.

- Type of account (Operating/Investment/Other (specify)
- Potential monthly account activity (US $ equivalents converted to local currency)

4.2 Address document (Proof of Address)

Either 1 or 2 shall be provided to prove the existing address:
1. One copy of an utility bill (e.g. electricity, water, gas, phone bill, mobile phone bill,)

2. Certificate of Residence, social insurance card, national ID card, driver's license (If passport is provided as the customer's ID), and other documents issued by local governments that ILEXEXCHANGE can recognize.

- The utility bill shall be issued within 3 months of the application date.
- The certificate of Residence shall be issued within 3 months before the
- submission. The valid term of 3 months is counted at ILEXEXCHANGE's receiving of the card.
- Each document shall clearly contain customer's name and address.

4.3 Change of ID/Address

If the contents of the ID are updated, the customer needs to contact to ILEXEXCHANGE to notify the change of the ID contents. Customer needs to notify the change of address through I-Account.

The submitted documents are not returned to the customers in any way. The conditions not stated in this policy will follow the other terms and conditions offered by ILEXEXCHANGE. ILEXEXCHANGE reserve the right to ask customers to provide other supporting documents for ID and address proof confirmation.

Partnerships

In the case of partnerships, where the partners or principles are not known to ILEXEXCHANGE the identity of the partners or principals should be verified as if they were personal customers using the same standards for personal clients.

In the case of partnerships, the standards are the same as that for corporations, except that instead of proving corporate validity and existence, the partnership's validity and existence is verified through:

- Partnership document form signed by all partners which confirms that name and term of the partnership;
- Operating/Trading Address;
- Business licenses if required;
- Proof of Trading Name (letterhead, tax receipt etc.); and
- Mail, Phone, Fax and E-mail addresses;

Personal identification must be on file for the signatories to the account and the managing partner(s)

4.5 Correspondent Banking Accounts – ILEXEXCHANGE will not accept correspondent banking or managed bank mandates.

4.6 Payable Through Accounts – ILEXEXCHANGE will not accept Payables through Accounts as defined by the United State Banking regulators.

4.7 7 Foreign Exchange Dealers/Cambios Accounts

a) ILEXEXCHANGE may offer payment services to high quality commercial customers, who maintain foreign exchange operations as a small part of its overall operations. Maintaining such accounts must be approved by CEO and may be cancelled at any time.

4.8 Unincorporated Entities. "Trading As" Accounts

In the case of Unincorporated Entities or "Trading As" Accounts, the client is the person or persons running the business. There is no legal distinction between the person and the business.

Consequently, the client acceptance procedures must be done on the person or persons conducting the business. In addition, the one or more of the following information should be obtained:

- Operating/Trading Address;
- Business licenses if required;
- Proof of Trading Name (letterhead, tax receipt etc.); and
- Mail, Phone, Fax and E-mail addresses;

Personal identification must be on file for the signatories to the account and managing partner(s).

4.9 Charities, Clubs and Associations – ILEXEXCHANGE does not routinely offer accounts for Charities, Clubs and Associations. In the event that accounts are to be opened for charities, clubs, and societies, ILEXEXCHANGE should take reasonable steps to identify and verify signatories along with the institution itseiLexExchange. The principals

who should be identified should be considered to be those persons exercising control or significant influence over the organization's assets. This will often include members of a governing body or committee, any board members, the Treasurer, and all signatories.
In all cases independent verification should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

Trusts and Foundations - When opening an account for a trust, ILEXEXCHANGE should take reasonable steps to verify the trustee(s), the settler(s) of the trust (including any persons settling assets into the trust), any protector(s), beneficiary(ies), and signatories. Beneficiaries should be identified when they are defined. Similarly for Foundations, in the event that such an account is to be opened, steps should be taken to verify the founder, the managers/directors and the beneficiaries – as per the policies as set out for Personal Accounts.

ILEXEXCHANGE must identify and establish the bona-fides of all parties to a trust using the standards established in this policy. Documents required include:

a) Nature and purpose of the trust;
b) Verification of the identity of the trustee, settler, protector, and person providing the funds, controller or similar person with the holding power to appoint or remove the trustee;
c) Source of the funds;

4.10 Professional Intermediaries - When a professional intermediary opens a client account on behaiLexExchange of a single client, that client must be identified in the same manner as others appropriate to the legal nature of the account.

4.11 Agent or Nominee Accounts
Where an account is being opened on behaiLexExchange of a minor or other third party, by a trustee, nominee, representative or any other third party, the identity of all the parties to the account must be known to ILEXEXCHANGE and fully investigated, including the beneficiaries.

4.12 Funds and Unit Trusts
Where such circumstances apply and an account is opened for an open or closed ended investment company, unit trust or limited partnership which is also subject to the same due diligence standards in respect of its client base, the following should be considered as principals to identify:

- the fund itseiLexExchange;
- its directors or any controlling board where it is a company;
- its trustee where it is a unit trust;
- its managing (general) partner where it is a limited partnership;
- account signatories;
- any other person who has control over the relationship; e.g. fund administrator or manager.

In addition all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.
Intermediaries should be treated as individual customers of ILEXEXCHANGE and the standing of the intermediary should be separately verified by obtaining the appropriate information drawn from the itemized lists as per other customers.

4.13 Occasional Customers (non-Account holders)
Funds deposited into an existing account by persons whose names do not appear on the mandate for that account, should be treated as follows.
ILEXEXCHANGE can only undertake transactions for non-account holders where there is satisfactory evidence of identity.

4.14 Politically Exposed Persons
Politically Exposed Persons are individuals who are, or have been entrusted with prominent public functions.
As a general rule, Politically Exposed Persons should not have a sound business reason for having accounts with ILEXEXCHANGE. Consequently, accounts with Politically Exposed Persons can only be undertaken and maintained with the approval of CEO.

Where ongoing due diligence reveals uncertainties about the legitimacy of funds, the business unit leader should review the relationship with the customer and make such unusual activity reports as are necessary.

4 Anti-Money Laundering Prevention

ILEXEXCHANGE will conduct its business in conformity with the highest ethical standards in the countries in which it does business, and will adhere to all laws and regulations pertaining to financial organizations. It is vital for all ILEXEXCHANGE customers, agents and employees and associates to fully understand those actions that may violate applicable AML or counter-terrorism statutes.

5.1 Monitoring Transactions

5.1.1 Declaration of Source of Funds Report

Money laundering laws require that records be kept of all business transactions. In most cases, there is sufficient information in the instrument evidencing the transaction, such as a check or wire transfer to provide the key information about the transaction (e.g. date amount, payer, payee, and source of funds – i.e. the bank account the check is drawn on). If a customer does not complete the required information fully, the deposit should not generally be accepted.

Staff are not expected however, to refuse to post a deposit, if in their opinion to do so, might expose the staff to a dangerous situation. In such cases, an unusual transaction report must be prepared and filed.

The AML officer - Controller and Compliance should maintain a money laundering reports database which includes information on all such reports. Over time tools should be developed that will give greater assurance that the declarations of source of funds reports match actual cash deposits taken at the branch level.

5.1.2 **Review by** the AML OFFICER **- Controller and Compliance**

On a regular basis, a Money Laundering Reporting Officer and the AML OFFICER - Controller and Compliance should review reports on significant deposits. This independent review will ensure that

- Systems reports that show account activity;
- Large Cash Deposit Reports;
- Kiting Reports;
- System Reports that reconcile Declaration of Source of Funds to Large Cash Deposit Forms and Exception Lists;
- Wire Transfer Logs; and
- Branch staff is identifying all significant deposits through transaction systems.

6 Obligation to Monitor Account Activity

Knowing Your Customer is an obligation that continues throughout the entire life of a relationship with a client. All staff at ILEXEXCHANGE has a legal obligation to monitor account activity for unusual activity that may be evidence of money laundering, credit or operational problems, or to identify sales or customer service opportunities.

In all jurisdictions that a financial institute does business, there is a legal obligation to report “suspicious transactions” to law enforcement. *Identification of potential suspicious transactions is the responsibility of all staff.*

6.1 Monitoring by Front Line Staff

Front line staffs who deal directly with customers are the primary defense in identifying and escalating unusual activity to management and compliance. At ILEXEXCHANGE, such front line staffs include:

- Service Representatives;
- Account Officers and Account Managers; and
- Registered Representatives;

Tools and processes that front line staff has to assist them in monitoring accounts include:

- Their observation and experience when directly interacting with customers;
- Checklists and procedures when opening accounts;

- Review of transactions before processing them; and
- System reports that show account activity.

6.2 Monitoring by Line Management

Managers, regardless of whether or not they operate in a Branch Money Laundering control capacity or not, are the second line of defense in identifying and escalating unusual activity to management and compliance.
Management includes:

- the compliance committee – Cards and Payments, and the AML OFFICER – Controller and Compliance,
- Banking Managers,
- Managers, Credit Cards and Payments

Tools and processes that management has to assist them in monitoring accounts include:

- Their observation and experience when directly interacting with customers;
- Signoff of account opening documentation for new accounts;
- Systems reports that list new accounts;
- Annual review of commercial and trust accounts;
- Approval of transactions before front line staff process them;
- System reports that show account activity;
- Large Cash Deposit Reports;
- Large Item Reports; and
- Kiting Reports.

6.3 Monitoring by the AML OFFICER **– Controller and Compliance**

the AML OFFICER – Controller and Compliance the third line of defense after front line staff and line management in identifying and escalating unusual activity to management and compliance.

Tools that AML OFFICER – Controller and Compliance have to monitor account activity include:

- Spot checking of compliance to account opening procedures;
- Systems reports that show account activity;
- Large Cash Deposit Reports;
- Kiting Reports;
- System Reports that reconcile Declaration of Source of Funds to Large Cash Deposit Forms and Exception Lists; and
- Wire Transfer Logs.

7 Unusual Activity

As the types of transactions that may be used for money laundering are almost unlimited, it is difficult to define a suspicious transaction in absolute terms. The key to understanding who the customer is and what is the normal range of transactions that the customer will legitimately undertake. Staff should be vigilant for transactions that fall outside the range of normal behavior. ILEXEXCHANGE employees should be encouraged to think of “unusual” activity. This is a lower standard than “suspicious”. Management and compliance should review the reports and determine whether the activity is truly suspicious and worthy of filing a report with the appropriate authority.

Unusual Activity may occur with business, trust or personal transactions that do not appear to be consistent with the manner in which you expect that account to operate. Unusual Activity includes all types of banking transactions, including: wire transfers, managers’ checks, non-cash deposits, trusts, loans, or security transactions. Unusual Activity may be a single transaction or a series of transactions. Unusual Activity may not be money laundering, but may be indications of fraud or other improper activity. Unusual Activity may also be just poor decisions on the part of our customers, which we should encourage them not to make as part of our sales and service activity. An Unusual Activity Report should have value beyond just preventing money laundering.

When determining whether or not a transaction is unusual, ILEXEXCHANGE should consider the following:

- Is the size of the transaction consistent with the normal activities of the Customer?
- Is the transaction rational based on what we know about the customer's personal or business activities?Has the pattern of transactions conducted by the customers changed?
- Where the transaction is a cross border one, does the customer have any obvious reason for conducting business with the country involved?

7.1 Examples of potential unusual activity

The following examples of potentially unusual activity may also include:

7.1.1 Use of Bank Account Transactions

- Customers who maintain a number of trustee or client's account that do not appear to be consistent with the type of business they conduct;
- Customers who have numerous accounts and pay cash into each of them, which in the total is a significant amount;
- Any individual or company account which shows little or no normal personal business, but is used to receive or disburse large sums which have no obvious relationship to the account holder and/or the business;
- Substantial increases in turnover in an account which cannot be explained by business activity or personal circumstances;
- A number of people who deposit many payments into the same account without a good reason;
- Large cash withdrawals from a previously dormant account or from an account which has unexpectedly received a large credit from abroad;
- Customer reluctance to provide normal information when opening an account, providing minimal or fictitious information, or when applying for an account provides information that is difficult or costly to verify;
- Customers who decline to provide information that normally would make the customer eligible for credit or other valuable banking services;
- Customers who appear to have accounts with several financial institutions, particularly when ILEXEXCHANGE is aware that these accounts are later consolidated in another account;
- Matching payments out with credits paid in cash on the same, or previous day;
- Paying in large, third party checks endorsed in favor of the customer.

7.1.2 of Lending Products

- Request to borrow against assets held by financial institutions or a third party, where the origin of the assets are not known or the assets are inconsistent with the customer's apparent wealth;
- Request by a customer to provide financing where the source of the customer's payment or collateral is not clear, in particular where property is involved.
- Customers who borrow and then repay unexpectedly and in particular, with problem loans.
- Customers requesting back to back deposit and loan transactions and in particular involving overseas financial institutions.

7.1.3 of Securities Transactions

- Purchasing securities to be held in safe custody that do not appear to be appropriate given the customer's apparent net worth;
- Request for securities or foreign exchange services where the source of funds is unclear or not consistent with the customer's apparent worth;
- Large or unusual settlement of securities transactions by cash; and
- Buying and selling of a security with no discernable purpose or in circumstances that appear unusual, for instance transactions that are designed specifically to create a loss.

7.1.4 General Concerns

- Transactions which have no apparent commercial purpose;
- Lack of information/documentation to support a transaction;
- Unable to obtain adequate comfort levels for the "Knowing Your Customer" issues;
- Transactions routed through unusual/unacceptable jurisdictions;

- Client has no interest in the performance of his investments and is willing to accept losses without question;Client is willing to pay far higher fees than would be expected for the level of services provided;
- Reluctance by client to provide information on receipts/deposits or offers reasonable answers but cannot produce back-up (e.g. commission agreements) when asked; and
- Rewards are offered to staff members for services rendered e.g. cash, gift vouchers, trips, dinner.

7.2 Reporting of Unusual Activities and Suspicious Transactions

7.2.1 Reporting to money laundering control officer

If you observe unusual activity in any transaction, you must inform the AML officer – Controller and Compliance immediately. Front line staff or account managers should first complete an Unusual Activity Report and pass it to their manager for review. The AML officer – Controller and Compliance should ensure the report is complete and that it explains what is unusual about the transaction.

You must keep the situation strictly confidential. Under no circumstances are you to tell the customer or anyone else that there has been an Unusual Activity Report. ILEXEXCHANGE and its staff have legal protection from criminal or civil liability when a suspicious transaction report is made to law enforcement.

7.2.2 Reporting of Suspicious Transactions to Local Law Enforcement

All suspicious activities reports should be submitted to the relative authority in New Zealand. If a member of a law enforcement agency contacts ILEXEXCHANGE, these requests must be directed to the AML officer – Controller and Compliance. Customer information can only be disclosed to law enforcement under very specific legal arrangement. In most cases, there is a court order that is authorizing the disclosure of information or ongoing monitoring of the account by law enforcement. While it most undoubtedly should be ILEXEXCHANGE policy to co-operate with law enforcement, it must ensure that such co-operation is done under proper legal process. Any co-operation with law enforcement will be done under the direction of the AML officer – Controller and Compliance.

You must keep the situation strictly confidential. Under no circumstances are you to tell the customer or anyone else that a customer is under investigation or an account if under a monitoring order. ILEXEXCHANGE and its staff have legal protection from criminal or civil liability when co-operating with law enforcement under such court orders and other specific legal and statutory arrangements.

ILEXEXCHANGE will notify the relative authority within two days of receiving any requests for information from law enforcement on a ILEXEXCHANGE prepaid card. Additionally, ILEXEXCHANGE will response with fourteen days of receiving requests for Information from the relative authority. ILEXEXCHANGE will respond to such requests according to its own legal guidance.

8. Sanctioned and Restricted Countries

ILEXEXCHANGE has designed a Restricted Country List, which has been established to meet OFAC and other Sanctions Risk. ILEXEXCHANGE reserves the right to add or delete countries from the restricted list depending on a number of factors, including but not limited to, sanctions programs established by OFAC or the United Nations, countries designated as non- cooperative or as special concern by FATF, or countries deemed to be unacceptable risk.

ILEXEXCHANGE is prohibited to conduct business with, or open accounts for, entities or persons listed on the SDN lists published by OFAC.

Screening Cardholders and Partners against the OFAC Lists

As part of its AML programme, ILEXEXCHANGE is required to screen all customers and partners against the OFAC lists. Screening must be done:

- Initially, prior to card issuance; and
- Monthly

ILEXEXCHANGE is required to keep a log of all potential OFAC hits, including the results of its efforts to clear the hit and whether the hit was a false positive or a valid match. ILEXEXCHANGE will be in a position to provide this OFAC log to the relative authority when it is requested.

ILEXEXCHANGE will immediately suspend the account and notify the relative authority of any validated OFAC

hits. Sanctioned and Restricted Countries

For countries listed on the Restricted Country List ILEXEXCHANGE is prohibited from:

- Issuing or mailing cards to customers with an address in, or an government ID from, the restricted country
- Allowing transactions to occur in the restricted country
- Doing business with a partner organized in, or located in, a restricted country

9. Ongoing Responsibilities

9.1 Training Obligations

ILEXEXCHANGE should establish and maintain programs for training of all employees, particularity staff assigned to handle transactions, customer service and wire transfer accounts, on a continuing basis.

- In addition, each new employee should be made aware of the concepts, procedures, and controls relative to anti-money laundering as part of their orientation process and to recognize the extent of their anti- money laundering responsibilities; for even though we talk in terms of ILEXEXCHANGE as a corporation, it should be recognized that it is individuals who drive these entities.

The following should be made available to all staff:

- Copies of ILEXEXCHANGE Anti-Money Laundering Policy, Procedures and Forms on Intranet and Local Area Networks;
- General Circulars;
- Business Unit training by management
- Visits by Compliance committee

9.2 2 Record Keeping Obligations

Under a ILEXEXCHANGE Retention of Records policy and under most local money laundering legislation key documents must be kept at least 1 year after the end of the relationship or the last occasional transaction.

Key documents to be safeguarded include:

- Account opening documentation;
- Each advice or instruction received or given regarding a transaction which results in the transfer of funds in the Threshold Amount;
- Each item, including checks, drafts or transfers of credit, of more than the Threshold Amount a person, account or place within or outside the jurisdiction;
- Each remittance or transfer of funds or currency of more than the Threshold Amount within or outside the jurisdiction;
- Each check, or draft in an amount in excess of the Threshold Amount drawn or issued by a financial institution which ILEXEXCHANGE has paid or presented to for payment;
- Each item in excess of the U.S. equivalent Threshold Amount received directly by letter, cable, or other means from a financial institution outside the jurisdiction;
- Each completed Declaration of Source of Funds report;
- Each completed Unusual Activity Report; and
- Each completed Suspicious Transaction Report.

10. Customer Education

Implementation of KYC procedures and AML policy requires ILEXEXCHANGE to demand certain information from the customers that may be personal or have never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, ILEXEXCHANGE needs to educate

the customer of the objectives of the policy. ILEXEXCHANGE shall explain the same condition anytime it gets the customer support request or inquiries and necessity of the submission of relevant documents.

11. Independent Testing

ILEXEXCHANGE AML program will be periodically tested for its effectiveness by an independent party, either internal or external. If internal, the person(s) conducting the review must be independent from the designated AML Officer and staff and must have enough knowledge of AML requirements to adequately perform the testing.